Commentaire de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel (2e partie)

IV. – Droits de la personne concernée

Les auteurs de la directive ont décrit de manière détaillée l'ensemble des droits reconnus au sujet des données ; non sans ambiguïté parfois.

Nous ne passerons pas ici en revue les droits traditionnels : accès, correction, action, si ce n'est peut-être pour émettre une réflexion sur le régime d'exception au droit d'accès.

Aux termes de l'article 15 de la directive (50), l'accès aux données peut être refusé pour certains motifs. Ces limitations ne sont cependant admises que pour les fichiers détenus par le secteur public et moyennant l'adoption d'une loi nationale. Cela conduit à deux observations.

Pourquoi avoir restreint le champ de ce régime d'exception au secteur public ? N'y a-t-il pas des cas dans lesquels le secteur privé devrait être légitimement en droit de s'opposer à une demande d'accès ? La disposition en question énonce, entre autres motifs de refus de l'accès, « un droit équivalent d'une autre personne (51) et des droits et libertés d'autrui » (52). Ces droits qui sont pris en considération par le secteur public ne peuvent-ils l'être par le secteur privé ? L'exposé des motifs mentionne, à titre d'exemple, la protection des secrets commerciaux. Il s'agit là d'intérêts par essence privés, et dès lors davantage en jeu au sein même du secteur privé. Ainsi, en certains cas, la simple connaissance par une personne ou une entreprise concurrente de l'existence d'un fichier reprenant des données de telle nature peut nuire au développement d'une firme. Il est donc à déplorer – ce que n'ont pas manqué de faire les acteurs privés concernés – que la possiblité de refus soit exclusivement réservée au secteur public.

Par ailleurs, la formule de la loi d'exception n'est viable spécialement en ce qui concerne les droits concurrents des personnes autres que le sujet de données que si pareille loi est exprimée en termes généraux (53). Dans le cas inverse, on verrait fleurir une multitude de textes législatifs qui, au demeurant, ne couvriraient pas la réalité entière et seraient par là insatisfaisants (sans parler des lenteurs, traditionnelles en certains Etats, du fonctionnement de l'appareil législatif).

En deux endroits, la directive évoque, en des termes différents et – on pouvait s'y attendre – contradictoires, un droit particulier qui fait craindre à première vue pour la liberté d'information. Il s'agit du droit qui appartient à l'individu concerné de s'opposer au traitement de ses données.

C'est au sein des dispositions portant sur les formalités à accomplir lors de la communication de données que l'on trouve la première affirmation de ce droit. Aux termes de l'article 9.3, en effet, « si la personne concernée objecte contre la communication ou *tout autre traitement*, le responsable du fichier est tenu de cesser le traitement contesté sauf si une disposition légale l'y autorise » .

On peut s'interroger sur l'exacte portée de cette disposition lorsqu'on la compare avec l'article 14.1 qui instaure le droit de s'opposer à un traitement pour raisons légitimes et l'article 14.6 qui prévoit un droit d'obtenir le retrait de certains fichiers. Avant tout, il est évident que l'article 9.5 n'a pas sa place parmi les dispositions relatives à l'obligation d'information du fiché lors de la communication de données le concernant. Il est à lire dans le cadre de l'article 14, panel des droits garantis aux sujets de données. Au-delà, on peut en contester le contenu. Il est clair que cet article ne peut donner au fiché un droit absolu de s'opposer à la communication ou à tout autre traitement lorsque ces communications ou traitements sont légitimes.

(50) L'article 15 prévoit que les Etats membres peuvent limiter par une loi les droits prévus aux points 3 et 4 de l'article 14 pour des motifs relatifs à :
(a) la sûreté de l'Etat, ou
(b) la défense, ou
(c) des poursuites pénales, ou
(d) la sécurité publique, ou
(e) un intérêt économique et financier impératif dûment justifié d'un Etat membre, ou de la Communauté, ou
(f) la nécessité de l'exercice des fonctions de contrôle ou d'inspection de l'autorité publique, ou
(g) un droit équivalent d'une autre personne et des droits et libertés d'autrui.

(51) Par « autre personne », il faut entendre les personnes autres que la personne concernée, catégorie qui englobe donc le responsable du fichier.

(52) Article 15(g) de la proposition de directive. Notons que le texte parle d'un « droit équivalent » d'une autre personne, sans exiger qu'il soit même supérieur.

(53) Dans la mesure où l'autorité de contrôle a un pouvoir de vérification des fichiers, sur simple demande de la personne concernée, les droits de cette dernière sont préservés.

N'existe-t-il pas un droit des entreprises (ou autres) à constituer des fichiers sans l'accord nécessaire de la personne concernée, dans la mesure où les fichiers sont conformes à l'article 8.1 (hypothèses de légitimité des traitements en l'absence de consentement du fiché) ? D'autant que si le traitement est admis sur base de l'article 8.1.C., c'est que l'intérêt légitime poursuivi par le responsable du fichier prévaut sur l'intérêt de la personne concernée. Il serait difficile dans cette hypothèse d'admettre qu'une objection non-motivée de l'individu fiché puisse mettre fin au traitement des données...

C'est à l'article 14.1 que ce droit, dépourvu cette fois de son caractère absolu, refait son apparition. La personne concernée se voit ainsi accorder le droit de s'opposer, pour des raisons légitimes, à ce que les données à caractère personnel la concernant fasse l'objet d'un traitement. Cette disposition est reprise de la loi française « Informatique et libertés » (54). Elle peut dès lors se lire à la lumière de l'interprétation qui en a été faite en France. L'exposé des motifs de la proposition de directive va d'ailleurs dans ce sens, lorsqu'il précise que « le droit de s'opposer pour des raisons légitimes est simplement le droit de contester la légitimité (licéité) du traitement d'une donnée par le ficheur » . En d'autres termes, il s'agit pour le fiché de mettre en cause la pertinence d'une donnée par rapport aux finalités d'un fichier. Il n'est donc pas question de déroger ici à l'article 8.1. C'est bien sûr à l'autorité de protection des données ou à la justice que reviendra le dernier mot pour définir les limites imposées par la finalité des fichiers.

Les auteurs de la proposition de directive ont inséré un droit nouveau dont il a été fait rapide mention dans le paragraphe qui précède, mais qui mérite, de par son caractère original, un regard plus long. La personne concernée est ainsi en droit « d'obtenir sur demande l'effacement sans frais des données la concernant enregistrées dans des fichiers de prospection commerciale ou publicitaire » (55).

Remarquons que dans la majorité des pays d'Europe existe déjà la possibilité pour les personnes concernées de demander le retrait de leurs nom et coordonnées de l'annuaire téléphonique. A ces « listes rouges », la France ajoute une liste orange qui permet aux abonnés non pas de s'exclure de l'annuaire, mais d'exclure l'utilisation à des fins commerciales ou publicitaires de leurs données. Cette solution, unique jusqu'ici, répond à la question : faut-il renoncer aux finalités téléphoniques (listes rouges) afin d'éviter toute utilisation pour d'autres finalités ?

La directive va encore plus loin puisqu'elle reconnaît le droit de se retirer de tout fichier de prospection commerciale ou publicitaire. En outre, contrairement à ce qui se pratique généralement en matière de télécommunications, l'individu doit pouvoir obtenir gratuitement l'effacement de ses données.

Dernier droit suscitant un commentaire, celui de « ne pas être soumis à une décision administrative ou privée impliquant une appréciation (du) comportement qui ait pour seul fondement un traitement automatisé de données à caractère personnel donnant une définition du profil ou de la personnalité de l'intéressé » (56).

Lui aussi inspiré du modèle français (57), ce droit garantit aux individus de ne pas se voir imposer une décision qui soit fondée sur le seul traitement automatisé de données. Il ne s'agit pas, par cette disposition, de remettre en cause l'existence des systèmes automatisés d'aide à la décision (notamment l'établissement de profils statistiques et actuariels d'usage quotidien dans les secteurs bancaire, de crédit et d'assurance), mais de refuser qu'une décision se prenne sans intervention humaine.

4. Données sensibles

A l'instar de la Convention du Conseil de l'Europe (58), la proposition de directive communautaire a pris le parti d'envisager isolément la problématique des données dites « sensibles ». Son article 17 soumet ainsi le traitement automatisé des données révélant l'origine raciale et ethnique, l'opinion politique, les convictions religieuses ou philosophiques, les appartenances syndicales et les informations relatives à la santé et à la vie sexuelle à un régime particulièrement restrictif. Ainsi, il érige en principe l'interdiction de tout traitement automatisé des données sensibles énumérées (59). Toutefois leur traitement est admis à titre exceptionnel pour autant que la personne concernée y consente ou qu'une loi nationale l'autorise. Le législateur communautaire, soucieux d'éviter que la disposition ne reste lettre morte par un trop grand formalisme législatif, a introduit une certaine souplesse en prévoyant le consentement de l'individu comme exception. Il s'est donc bien gardé de réserver au seul législateur l'appréciation quant à l'opportunité de déroger à l'interdiction. Une heureuse initiative.

Attachons-nous, dans un premier temps au choix du législateur communautaire de réserver un sort particulier aux catégories de données reprises en l'article 17 du projet de directive. S'il apparaît que pareil choix s'en réfère encore à la nature particulièrement sen-

(54) Article 26 de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.*, 7 janvier 1978, rectificatif, *J.O.*, 25 janvier 1978.

(55) Article 14.6 de la proposition de directive.

(56) Article 14.2 de la proposition de directive.

(57) Article 2 de la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(58) L'article 6 de la Convention 108 du Conseil de l'Europe subordonne le traitement de certaines catégories particulières de données à l'adoption de « garanties appropriées ».

(59) La liste de données sensibles établie par le projet de directive est tout à fait identique à celle du projet de loi belge en la matière.

sible des informations mentionnées, ce n'est cependant plus l'idée de la nécessité de préserver un noyau dur de la vie privée qui gouverne le régime mis en place. Le législateur communautaire semble en effet avoir été davantage conscient du risque de discrimination que le traitement de telles données peut engendrer (60).

Néanmoins, le choix d'établir une liste « exhaustive » des données sensibles ne nous paraît pas des plus pertinents. Bien que, plusieurs législations étrangères aient succombé à cette tentation (61), il est édifiant de constater que le contenu des listes ainsi établies diffère sensiblement d'un pays à l'autre (62). Une attitude pragmatique conduit dès lors à conclure que le caractère sensible ou ordinaire d'une donnée ne s'apprécie pas dans l'absolu mais au vu de son contexte d'utilisation.

En outre, nous sommes d'avis que le traitement d'une donnée sensible doit être apprécié selon une démarche identique : la légitimité de son enregistrement et de son stockage doit être éprouvée à la lumière de la finalité poursuivie. Les auteurs du projet auraient dès lors dû préférer l'application stricte du principe de pertinence (63) à une énumération limitative de données prohibées. Dans un louable effort de tempérer un principe d'interdiction par trop absolu, ils ont bien tenté d'y introduire une certaine souplesse en autorisant d'y déroger moyennant le consentement de l'individu ou l'autorisation du législateur national (64). Outre le recours à une technique législative critiquable en soi, la référence au consentement de l'individu en tant qu'instrument dérogatoire n'équivaut à coup sûr pas à une application stricte du principe de finalité. Nul ne peut en effet assurer que l'individu sera toujours le mieux à même d'apprécier la pertinence du traitement d'une donnée voire même qu'il se trouve dans la meilleure position pour refuser, s'il le juge opportun, son consentement au traitement d'une donnée. Il nous faut faire confiance à l'individu, mais est-il bien vrai que ce dernier disposera dans chaque cas d'une information réellement adéquate ainsi que de la liberté et du recul suffisants pour apprécier la portée et les implications concrètes de son consentement ?

Toutefois, la problématique propre à la notion de « consentement » n'en demeure pas moins délicate. Ainsi, le recours à un consentement particulier peut surprendre, tant celui dont question à l'article 17 paraît offrir moins de garanties que le consentement informé, spécifique, exprès et rétractable du régime commun (voir *supra* 3.C.1) (65).

Examinons les caractéristiques du consentement requis en matière de traitement des données sensibles. L'article 17 (66) stipule que le consentement doit être libre. Cette exigence n'est-elle point superflue dans la mesure où il s'agit là d'une condition de validité propre à tout consentement ? Par ailleurs, le caractère exprès n'ajoute rien de neuf puisqu'il était déjà repris à l'article 12. Enfin, l'article 17 requiert un consentement écrit. S'il est incontestable que l'écrit offre une plus grande sécurité en matière de preuve et qu'il rend l'émission de la volonté plus solennelle, il ne se substitue pas à l'exigence d'un consentement rétractable ou informé. Le silence de l'article 17 comporte dès lors le risque que l'individu soit abusé car il est appelé à consentir, sans autre forme de dédit, à un traitement dont il n'est parfois pas en mesure d'apprécier les risques ou avantages. Ce constat amène à la conclusion que le consentement prévu à l'article 17 doit être interprété à la lumière du consentement prévu par l'article 12, tout en requérant un support écrit spécifique (67).

Parallèlement à la dérogation consensuelle dont il vient d'être question, le législateur communautaire a également prévu la possibilité de se soustraire à l'interdiction d'enregistrer des données sensibles en vertu d'une loi nationale. Cette seconde dérogation fait, elle aussi, l'objet d'une attention spécifique et sa mise en œuvre est sévèrement réglementée. Ainsi, seuls des motifs d'intérêt public importants peuvent justifier l'intervention du législateur national, qui se doit, en outre, de préciser les types de données sensibles traitées, les personnes ayant accès aux données, les garanties appropriées contre les utilisations abusives ainsi que les autorisations d'accès.

L'efficacité de cet instrument dérogatoire n'en demeure pas moins sujette à caution. Le pouvoir législatif, bien que constituant formellement le garant idéal de la liberté démocratique, n'est-il pas souvent victime d'un carcan procédural et d'enjeux politiques ? Ainsi, ne risque-t-on pas de voir certaines activités paralysées aussi longtemps que le législateur n'adoptera pas une réglementation adéquate ou, au contraire, de voir les Parlements nationaux contraints de voter des lois « mammouth » qui autoriseraient le traitement de données sensibles dans le chef de très larges catégories d'utilisateurs mal ou trop largement identifiés.

Enfin, il nous est permis de nous interroger, sur le contenu de la notion de « motif d'intérêt public important » (68). A titre illustratif, nous pouvons utilement nous référer à la loi française (69). Elle aussi, connaît une disposition similaire par laquelle il est permis, sur « proposition ou avis conforme de la Commission (et par voie de) décret (pris) en Conseil d'Etat » (70), de déroger à l'interdiction d'enregistrer des données sensibles pour des motifs d'intérêt public . Les seuls motifs d'intérêt public admis jusqu'à présent par la CNIL concernent les traitements de données organisés par le secteur public (71). En outre, chaque exception fait l'objet d'une étude spécifique qui apprécie au cas par cas, compte tenu de la population concernée, les finalités poursuivies et les risques particuliers encourus par les libertés. Nous observons dès lors qu'en France la possibilité de déroger à l'interdiction sur base d'une loi ne joue qu'à l'égard de fichiers publics. Pareille solution risque de se révéler trop contraignante lorsqu'il s'agira d'évoquer l'article 17 du projet de directive communautaire. Pouvons-nous en effet réserver sans autre forme de procès, la notion de motif d'intérêt public aux seuls fichiers publics ?

Enfin, le législateur communautaire opère une nouvelle distinction parmi les données sensibles, en constituant une sous-catégorie propre aux données portant sur des condamnations pénales. Pour cette nouvelle catégorie, il prévoit un régime spécifique détaillé à l'article 17, § 3. La proposition de directive n'autorise en effet la conservation de cette catégorie de données que dans des fichiers relevant du secteur public. La disposition gagnerait toutefois à voir son champ d'application étendu à d'autres données dont la conservation pourrait également se révéler lourde de conséquences pour la personne concernée. Nous pensons tout particulièrement au sort des données relatives à un acquittement ou un sursis ou même à la seule existence d'une instruction judiciaire. Nous pouvons, à cet effet, en référer à nouveau à la législation française qui réserve également aux seules autorités publiques agissant dans le cadre de leurs attributions, et sous réserve d'un avis conforme de l'autorité nationale de protection des données, ou aux personnes morales gérant un service public, l'enregistrement des informations concernant les condamnations de même que les infractions et mesures de sûreté (72).

Par ailleurs, le choix du législateur communautaire de restreindre aux seuls fichiers publics la conservation des données portant sur des condamnations pénales nous paraît peu opportun. Il est entendu qu'une attitude permissive à l'égard de la conservation de ces données pourrait engendrer des situations préjudiciables, mais fallait-il pour autant exclure toute possibilité de conservation de données judiciaires dans le chef du secteur privé (73) ? D'une part créer une sous-catégorie parmi les données sensibles nous semble critiquable. D'autre part, l'opération de conservation des données est par définition comprise dans le traitement (74). Sa légitimité doit donc être appréciée de la même façon à savoir au regard de la finalité poursuivie.

5. Qualité des données

L'article 16 du projet de directive reprend les grands principes de qualité des données tels qu'ils ont déjà été énoncés à l'article 5 de la Convention du Conseil de l'Europe. Ainsi, il est prévu que la collecte et le traitement des données doivent être effectués loyalement et licitement et, parallèlement, que l'enregistrement, le traitement et la conservation des données doivent respecter le principe de finalité. Ce dernier principe suppose d'une part que les données soient enregistrées, utilisées et conservées pour des finalités déterminées (75), explicites (76) et légitimes (77) et d'autre

(60) Y. Poullet, « Informatiques et libertés : un débat en quête de solutions », *La Semaine Informatique*, 1990, n° 184, p. 41 ; CNIL, *Dix ans d'informatique et libertés*, Economica, Paris, 1988, p. 42.

(61) Voir par exemple l'article 31 de la loi française, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés ; l'article 7 de la loi néerlandaise du 28 décembre 1988 (wet persoonsregistratie), *Staatsblad*, 1988, p. 665 ; l'article 7 du projet de loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ; les sections 6 et 9 de la loi norvégienne sur les registres de données à caractère personnel et la section 4 de la loi suédoise sur les données à caractère personnel.

(62) Ainsi par exemple, les lois danoise et norvégienne considèrent les informations concernant la vie sexuelle comme manifestement sensibles. A l'opposé, la loi française ne prévoit pas de mesures particulières pour le traitement de telles données. La même disparité entre les législations nationales se retrouve également en ce qui concerne l'appartenance à une organisation syndicale.

(63) Le principe de finalité, bien que mal mis en valeur par l'agencement formel du texte est énoncé à l'article 16 du projet de directive.

(64) Il serait préférable de s'attacher à mieux définir les contours du principe plutôt que de jouer sur les exceptions.

(65) Le régime commun, c'est-à-dire la nécessité du consentement préalable à tout traitement, est prévu à l'article 8.1 (assorti de très larges exceptions), le consentement en tant que tel est défini à l'article 12.

(66) Le § 1 de l'article 17 prévoit que « les Etats membres interdisent le traitement automatisé, sauf accord libre, exprès et écrit de la personne concernée, des données révélant l'origine raciale et ethnique (...) ».

(67) Voy.. notamment la formulation même de l'article 12 définissant les conditions de validité du consentement *au sens* de la directive.

(68) Le § 2 de l'article 17 énonce que « les Etats membres peuvent prévoir pour des motifs d'intérêt public importants des dérogations aux dispositions du paragraphe 1 sur la base d'une loi précisant les types de données enregistrables, les personnes ayant accès au fichier ainsi que les garanties appropriées contre les utilisations abusives et les accès non autorisés ».

(69) Article 31 § 3 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et au libertés.

(70) La commission en question est la Commission Nationale Informatique et Libertés (C.N.I.L.), autorité française de protection des données.

(71) C.N.I.L., *Dix ans d'informatiques et Libertés, op. cit.*, p. 43.

(72) Article 30 de loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(73) Il est assez paradoxal que de manière générale les données judiciaires fassent justement l'objet d'une publicité organisée.

(74) L'article 2d du projet de directive définit le traitement comme les opérations effectuées ou non à l'aide de procédés automatisés: enregistrement, conservation...

(75) Aux termes de l'exposé des motifs, l'objet de l'enregistrement des données doit être déterminé, « c'est-à-dire que le but de l'enregistrement et de l'utilisation des données doit être défini et spécifié de façon aussi précise que possible ».

(76) Toujours suivant l'exposé des motifs, la finalité de l'enregistrement doit être spécifiée avant l'enregistrement des données et une modification ultérieure de la finalité du traitement n'est légitime que si elle n'est pas incompatible avec la finalité initiale.

(77) L'exposé des motifs précise encore que les finalités légitimes potentielles d'un fichier sont limitées : elles doivent être compatibles avec les dispositions du projet de directive et les législations nationales des Etats membres. En outre, en ce qui concerne les fichiers publics, les seules finalités légitimes sont celles qui correspondent aux fonctions administratives des responsables du fichier tandis que pour le secteur privé, il doit s'agir de finalités s'inscrivant dans le domaine d'activités commerciales des responsables de fichiers.

part que les données soient adéquates, pertinentes et non excessives au regard de ces finalités. Nous ne pouvons à nouveau que regretter, ainsi que ce fut dit précédemment à propos du principe de finalité, que des principes aussi fondamentaux ne soient pas posés dès les premiers articles du projet.

Indépendamment même de leur importance qui serait ainsi soulignée par l'architecture interne du texte de la directive, la logique intellectuelle et juridique emporte que les principes soient clairement énoncés avant d'être traduits de manière concrète. Ainsi, lorsque l'article 13 fait part d'une obligation d'information lors de la collecte des données, en réalité, il traduit simplement le principe de collecte des informations par des moyens loyaux et licites. Nul doute que la proposition gagnerait en crédibilité et en efficacité si son ordonnancement se révélait plus respectueux de sa propre logique (78).

6. Flux transfrontières de données

Les flux transfrontières de données personnelles à destination de pays tiers à la Communauté européenne font l'objet d'une attention toute particulière de la part des auteurs du projet de directive. La proposition entend ériger en principe, l'interdiction de tout transfert de données vers les Etats tiers si ces derniers ne leur assurent pas un niveau de protection adéquat (A). Le texte prévoit cependant certaines dérogations à ce principe de base (B).

L'originalité de la démarche communautaire mérite d'être soulignée car elle se distingue nettement de celle adoptée dans la Convention du Conseil de l'Europe. Lors de l'élaboration de cette Convention, les Etats membres du Conseil de l'Europe prirent le parti de ne traiter des questions de flux transfrontières de données qu'entre les seuls Etats contractants, et n'abordèrent pas les questions de transmission de données vers les pays tiers à la Convention. Un Etat partie prenante à la Convention demeure par conséquent parfaitement libre d'exporter des données vers un pays qui n'y a pas adhéré. Un tel choix implique bien des dangers en l'absence de toute garantie quant au régime de protection mis en œuvre par ce pays tiers. A l'inverse, rien n'interdit bien entendu l'Etat exportateur de mieux contrôler ces flux ni même de les interdire souverainement (79).

En vérité, la volonté du législateur – tant national que communautaire – d'assujettir les données à une réglementation limitant leurs possibilités d'exportation s'appuie généralement sur deux types de préoccupations. La première tend à éviter que les mesures de protection instaurées au sein d'un Etat ne soient affaiblies par des traitements effectués dans un pays tiers dont la législation plus libérale favoriserait la création d'un « paradis de données » (80). Concrètement, le péril naît d'une liberté absolue reconnue aux responsables de fichiers ressortissant de la Communauté européenne d'exporter les données à caractère personnel vers des Etats tiers, une liberté qui pourrait bien les conduire à « délocaliser » leurs fichiers en vue de les soustraire aux dispositions contraignantes de la directive.

La seconde préoccupation n'est pas liée à la qualité de la protection accordée aux données par le pays tiers mais dénote de la volonté d'un pays d'éviter que le traitement de renseignements concernant une large part de sa population ne soit effectué dans des entreprises situées à l'étranger (81). Un traitement à grande échelle effectué hors des frontières constituerait une menace pour l'intérêt national. Cette deuxième préoccupation apparaît toutefois absente des motivations propres à la démarche du législateur communautaire ; ce dernier semble en effet avoir été davantage sensible à prévenir tout détournement de la protection communautaire par le biais de traitements réalisés dans des pays tiers moins soucieux de la vie privée des individus.

Fidèle à la logique de son projet, le législateur communautaire entend pallier au mieux son impuissance face aux autorités nationales étrangères qui échappent à son contrôle pour des raisons évidentes tenant à la souveraineté étatique. Cette action préventive se traduit dans la proposition de directive par une stricte réglementation de l'exportation des données personnelles. Il requiert en effet, en son article 24, alinéa 1, que les législateurs nationaux érigent en principe que le transfert temporaire ou définitif de données faisant l'objet d'un traitement ou collectées en vue d'un traitement ne peut avoir lieu que pour autant que le pays importateur leur assure un niveau de protection « adéquat » .

A. – Principes de base (article 24)

Il convient avant de commenter et de nous prononcer quant au bien-fondé de l'approche communautaire, d'exposer la procédure mise en place. Les Etats membres incluront dans leur législation une disposition interdisant le transfert de données vers des Etats ne leur assurant pas un niveau de protection adéquat (82).

Il reviendra dans un premier temps aux Etats membres d'établir le caractère adéquat ou non de la protection accordée aux données par le pays tiers importateur en vue de limiter le cas échéant les flux transfrontières à destination de ce dernier. Les Etats membres devront évaluer le niveau de protection assuré par les pays tiers vers lesquels des exportations ont lieu. Le texte ne précisant pas les moyens devant être utilisés à cet effet, les Etats membres sont donc libres de choisir le système qui leur semble le plus approprié. Cependant, il apparaît en toute logique qu'au sein de chaque Etat membre, le pouvoir décisionnel reviendra à l'autorité de protection de données puisque celle-ci sera amenée à connaître des communications de données et notamment de celles destinées à l'étranger (83).

Si l'Etat membre estime la protection adéquate, il devrait normalement avaliser le transfert (voir *infra*). A l'opposé, s'il estime que la protection offerte par le pays tiers n'est pas adéquate, il bloquera le transfert et en informera la Commission (84).

C'est sur la base de ces informations fournies par les Etats membres, ou éventuellement à partir d'autres renseignements, que la Commission sera amenée à *constater* que le pays en question *ne dispose pas d'un* niveau de protection adéquat. Elle pourra alors entamer des négociations en vue de remédier à la situation. Le troisième paragraphe de l'article 24 pose une condition préalable à l'amorce de négociations : la situation doit être préjudiciable, que ce soit aux intérêts de la Communauté ou ceux d'un Etat membre. Le texte du projet ne précise cependant pas si les négociations doivent être menées avec le pays tiers ou avec l'Etat membre ou avec l'un et l'autre ou au choix selon les cas. L'exposé des motifs ne mentionnant que des négociations entre la Commission et le pays tiers concerné, on peut penser que c'est cette situation que le texte a voulu rencontrer.

Ajoutons que l'information communiquée par le pays à la Commission devrait être répercutée auprès des autres Etats membres en vue de suspendre tout transfert similaire de données (voir *infra*).

La procédure de l'article 24 prévoit enfin que la Commission pourra décider qu'un pays tiers offre bien une protection adéquate. Pour ce faire, elle prendra l'avis du comité consultatif et elle fondera son appréciation sur les deux critères suivants : l'état de la législation interne et l'existence d'engagements internationaux souscrits par l'Etat en question.

Certains commentaires spécifiques peuvent être émis tant en ce qui concerne la portée du concept « adéquat » (1), que l'étendue du pouvoir de décision des Etats membres (2) et les interactions entre ce pouvoir décisionnel et celui de la Commission (3).

1. Concept « adéquat »

L'évaluation du caractère adéquat de la protection présentée par un pays tiers risque de se révéler particulièrement délicate. La notion même de protection « adéquate » était inconnue jusqu'ici. La Convention du Conseil de l'Europe avait retenu, pour sa part, une approche s'appuyant sur le concept de protection équivalente. Ainsi, tout en érigeant en principe la libre circulation des données, la Convention admet que des restrictions (85) puissent être apportées en l'absence de protection équivalente dans le chef du pays importateur de données (86). La détermination de critères d'appréciation de ce dernier concept a déjà donné lieu à de nombreuses discussions et controverses (87). D'aucuns se sont notamment demandé si l'équivalence de la protection offerte devait être évaluée de façon globale à l'égard d'un pays déterminé ou s'il fallait l'évaluer au cas par cas en fonction du flux particulier posant problème.

A première vue, la notion de protection adéquate semble, quant à elle, faire référence à une exigence de protection moindre. Le texte du projet de directive ne fournit que peu d'indications relatives aux critères de décision : l'appréciation du caractère adéquat pourra en particulier se fonder sur les engagements internationaux souscrits par le pays tiers importateur de données ou sur base de la législation nationale de ce dernier.

Le premier critère repose sur l'adhésion du pays importateur à des normes internationales. A la lumière d'un premier tour d'horizon, seule la ratification de la Convention du Conseil de l'Europe (88) nous apparaît comme constitutive d'une preuve suffisante en soi, mais peut-il en être de même de la simple adhésion aux lignes directrices du Conseil de l'OCDE (89) ?

Le second critère s'appuie sur l'évaluation de la législation nationale. Les difficultés auxquelles ont donné lieu la compréhension du concept de protection équivalente resurgissent ici. Deux interprétations procédant de démarches différentes sont envisageables. D'une part, l'évaluation peut procéder d'une appréciation globale de la réglementation du pays destinataire des données ou, d'autre part, de la

(78) Obligation d'information lors de la collecte énoncée à l'article 13 du projet de directive.

(79) B.W. Napier, « Contractual solutions to the problem of equivalent data protection in transborder data flow, compte-rendu de la conférence des 27 et 28 mars à Luxembourg, p. 17.

(80) Voy. sur cette question F. Rigaux, « Le régime des données informatisées en droit international privé », *Journal de droit international*, 1986, pp. 311-328.

(81) Voy. également F. Rigaux, « Le régime des données informatisées en droit international privé », *op.cit.*

(82) Article 24, § 1 de la proposition de directive.

(83) Voy. art. 6.3 de la proposition de directive en ce qui concerne les traitements du secteur public et 11.1 pour ceux du secteur privé.

(84) Article 24, al 2 de la proposition de directive.

(85) Voy. les articles 3 (2) (a), 12 (3) (a).

(86) Les législations française, allemande, hollandaise et anglaise contiennent également des dispositions permettant de restreindre le libre-échange d'informations.

(87) Voy. L. Early, « Securing equivalent protection among nations in the context of transborder data flow: a possible role for contract law (the standard contract proposed by the Council of Europe », *Droit de l'informatique et des télécoms*, 1990, 4, pp. 10-14.

(88) L'exposé des motifs reprend explicitement la convention du Conseil de l'Europe à titre d'exemple des engagements que la Commission prendra en compte.

(89) La ratification de la Convention du Conseil de l'Europe implique que le pays en question ait adopté une législation nationale et donc que les deux critères d'appréciation formulés dans le texte du projet soient réunis.

volonté de retrouver la trace des principes de base de la proposition de directive dans le droit national du pays soumis à l'appréciation.

Si nous nous référons à la première possibilité, à savoir l'appréciation globale de la réglementation du pays destinataire des données, l'interprétation que donneront les Etats membres et la Commission du caractère adéquat de la protection mise en œuvre par le pays tiers, court le risque d'être particulièrement laxiste en raison d'impératifs politiques et économiques. Pratiquement, nous imaginons difficilement que l'un ou l'autre Etat membre ou la Commission estime de manière globale que la législation d'un pays comme les Etats-Unis n'offre pas un niveau de protection adéquat. Ce dernier Etat, pourtant, privilégie une approche sectorielle (90).

Le paradoxe de ce dernier constat illustre l'intérêt d'une autre approche. Ainsi, la notion de protection « adéquate » peut également être comprise comme se référant à l'existence dans un pays tiers d'une protection des données qui reprenne les principes de base de la proposition de directive. Le système mis en œuvre par le pays tiers aboutirait à une protection similaire à celle instaurée dans la Communauté, bien que les moyens utilisés à cet effet diffèrent sensiblement. La protection établie pourrait prendre diverses formes : sans revêtir nécessairement l'aspect d'une loi générale de protection des données, elle pourrait par exemple être constituée de réglementations spécifiques à un secteur (91), voire même être assurée par le biais de codes de bonne conduite. L'approche communautaire s'apparenterait donc, selon cette évaluation, plutôt à une approche sectorielle de la notion de protection adéquate. Cette démarche empreinte de pragmatisme nous paraît devoir être retenue car elle permet une appréciation plus fine et plus nuancée et, par là-même, favorise la mise en oeuvre de la disposition. Il ne s'agit en effet pas de condamner de manière globale la politique adoptée par un pays en matière de protection des données mais plutôt d'apprécier la protection offerte par cet Etat dans un secteur déterminé.

Notons encore à cet égard que la notion de protection adéquate se prête à une appréciation toute subjective. Si nous nous référons au sens usuel du terme adéquat, nous apprenons qu'il signifie approprié, ajusté à son but. La protection requise ne serait-elle donc point susceptible de vérification objective ?

(90) Les fichiers privés font l'objet de règles particulières généralement applicables à un secteur professionnel déterminé, voy. par exemple, le Fair Credit Reporting Act (1970) (Public Law, n° 91.508, 15 U.S.C. §§ 1681-1681 t) amendant le Consumer Credit Protection Act.

(91) « EC launches data protection Initiative », *T.D.R.*, oct. 1990, p. 6.

2. Pouvoir de décision des États membres

Jusqu'à présent, nous n'avons évoqué la notion de « niveau de protection adéquat » qu'en tant que concept litigieux et négatif. Toutefois, il est légitime de s'interroger également quant à l'attitude qui devra être adoptée par les Etats membres dans le cas où ils estiment que le pays tiers offre bien une protection adéquate aux données. Seront-ils dès lors tenus d'autoriser le transfert ? Le principe préconisé par la proposition de directive est celui de la possibilité et non de l'obligation de transmettre les données si le pays tiers présente une protection adéquate. Les Etats membres conservent donc l'entière liberté d'adopter une attitude libérale ou, au contraire, d'opposer encore certaines restrictions aux mouvements transfrontières.

3. Interactions États membres – Commission

La question de l'interaction entre le pouvoir décisionnel des Etats membres et celui de la Commission appelle quelques commentaires.

Avant tout, nous devons nous demander si la décision prise par la Commission qu'un pays tiers assure un niveau de protection adéquat s'imposera en tant que telle aux Etats membres. Par ailleurs, qu'adviendra-t-il lorsqu'un Etat estimera le niveau de protection offert adéquat tandis qu'un autre aura une opinion divergente sur la question ? L'Etat membre qui aura rendu un avis négatif sur le caractère adéquat de la protection entraînera-t-il à sa suite tous les autres Etats membres ? Le pays ayant émis un avis positif sera-t-il également tenu d'interdire l'exportation à destination de ce pays tiers ?

En principe, sous peine de vider la disposition de son sens, la seule notification à la Commission par un Etat membre de l'inexistence dans un pays tiers d'un niveau de protection adéquat devrait entraîner le blocage provisoire des flux de données à partir de tout pays membre de la CE. En effet, à défaut d'une telle interprétation, le risque est grand de voir l'exportateur choisir de faire transiter les données par un autre Etat membre de la CE dont l'appréciation serait plus laxiste. Si ce pays de transit membre de la Communauté a correctement traduit la directive dans son droit national, le pays dont l'exportateur des données est un ressortissant ne pourra restreindre les possibilités d'exportation. En effet, la directive interdit formellement les restrictions entre Etats membres au nom de la protection des données (92). En outre, elle ne connaît pas de disposition similaire à celle de la Convention du Conseil de l'Europe visant à pallier le risque de recours à pareille pratique. L'article 13, 3°, b de cette Convention dispose que, si un Etat adopte

(92) Article 1 § 2.

une politique libérale de transfert de données vers des Etats non parties à la Convention, cette situation peut justifier une restriction des flux de données à destination de cet Etat, paralysant de la sorte la liberté d'information garantie par sa ratification.

On peut interpréter la procédure mise en place à l'article 24 comme une réponse à pareille difficulté. En effet, elle devrait déboucher sur une politique communautaire en matière de flux transfrontière avec un large pouvoir de décision en la matière reconnu à la Commission.

Ainsi, si un Etat estime que la protection est non adéquate, il en avertit la Commission. Celle-ci peut également constater ce fait sur la base d'autres informations, sans avoir été saisie par un Etat membre. Suite à cette constatation et pour autant que la situation soit préjudiciable, la Commission est habilitée à mener des négociations. La notion même de « situations préjudiciables aux intérêts de la Communauté ou d'un Etat membre » (93) ne nous paraît d'ailleurs pas des plus claires. Ici encore, il appartiendra à la Commission de trancher sur cette question, préalable indispensable à l'amorce de négociations avec un pays tiers.

En outre, la Commission pourra décider en dernier recours, d'elle-même, bien qu'ayant pris *l'avis* du comité consultatif, qu'un pays tiers assure un niveau de protection adéquat.

La procédure nous semble bien aboutir à octroyer l'essence du pouvoir décisionnel à la Commission. Toute interprétation différente, qui ne s'appuyerait plus sur le concept d'unité du pouvoir décisionnel, conduirait à une situation d'autant plus préjudiciable que la directive ne comporte pas de disposition visant à empêcher les transferts par l'intermédiaire d'un pays membre vers un pays tiers ne présentant pas le niveau de protection requis. Suffira-t-il dès lors qu'un seul pays estime que la protection accordée n'est pas adéquate et en avertisse la Commission ou que la Commission le constate par elle-même ou décide au contraire que les garanties sont tout à fait acceptables, pour que l'ensemble des pays européens quelle que soit leur propre estimation du caractère adéquat de la protection offerte, soient tenus de se conformer à pareille décision ?

Rappelons à ce stade qu'un pays ne pourra en principe transférer de données à caractère personnel vers un pays tiers que si ce dernier assure aux données en question un niveau de protection adéquat (94). L'article 25 du projet de directive adoucit toutefois quelque peu la rigidité de ce principe d'interdiction.

(93) Article 24, § 3.

(94) L'Etat exportateur disposera normalement d'une législation nationale de protection des données conforme à la directive.

B. – Dérogations (article 25)

L'Etat membre hôte du fichier peut autoriser le transfert « sur présentation par le responsable du fichier de justifications suffisantes pour garantir le respect d'un niveau de protection adéquat » (95). Il ne s'agit pas à proprement parler de l'application extra-territoriale de la directive mais bien de l'obligation à charge de l'exportateur européen, d'assurer contractuellement la protection de la vie privée lorsque les données sont traitées à l'étranger.

L'article 25 prévoit une procédure d'information de la Commission et des Etats membres avec un délai de notification d'opposition de 10 jours. En cas de notification d'opposition, la Commission pourrait prendre les mesures appropriées et notamment aux termes de l'exposé des motifs, décider d'interdire le transfert (96).

La question qui surgit d'emblée est de déterminer si l'inclusion de clauses contractuelles d'adhésion aux principes de protection des données dans le contrat conclu entre l'exportateur et l'importateur de données suffira à assurer aux données une protection suffisante.

Nous ne pouvons en effet passer sous silence l'inconvénient majeur propre au recours aux clauses contractuelles de garantie, à savoir l'absence à la cause de l'individu fiché. Ce dernier, dont nous ne pouvons nier l'intérêt à l'égard de ces questions, n'étant pas partie au contrat passé entre le fournisseur et le destinataire des données, ne pourra faire valoir aucun droit ni introduire de recours dans l'hypothèse d'une utilisation erronée ou abusive des données. En vue de remédier à cet état de choses, le contrat devrait en tout état de cause inclure une clause assurant un droit d'accès et de correction dans le chef de l'individu concerné par les données.

Une seconde difficulté apparaît alors. Pour que les individus fichés jouissent d'une protection réellement efficiente, il est important de leur offrir des possibilités

(95) Le recours à des clauses contractuelles – reprenant les principes de protection des données de la Convention du Conseil de l'Europe et de la loi française du 6 janvier 1978 et notamment reconnaissant des droits d'accès et de rectification aux personnes concernées – avait déjà été imposé par la CNIL française dans l'affaire FIAT. Il s'agissait en l'espèce de transmission d'informations relatives aux cadres supérieurs entre FIAT France et FIAT Italie ; délibération n° 89-78 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres supérieurs de la société FIAT France à la société FIAT à Turin. La CNIL a fait application des mêmes principes dans d'autres affaires (informatisation du Centre de Sécurité Sociale des Travailleurs Migrants, délibération n° 89-98 du 26 septembre 1989 : Eurocode).

(96) La Commission est tenue de prendre l'avis du Comité consultatif selon la procédure prévue à l'article 30 § 2.

de recours s'inscrivant dans le cadre de la législation « privacy » de leur pays en cas d'utilisation abusive des données à l'étranger (97). Comment assurer aux autorités chargées de la protection des données un réel pouvoir hors des limites géographiques de leur compétence *rationae loci* (98) ? Seule la mise en place d'une procédure de contrôle *a priori* du contenu des données exportées nous paraît pouvoir rencontrer les impératifs de cette problématique.

Enfin, l'adoption d'une exception supplémentaire autorisant le transfert vers un pays ne garantissant pas un niveau de protection adéquat, exception basée sur le consentement de l'individu doit-elle être envisagée ? Reconnaître une telle exception permettrait de transférer des données personnelles dans le cas où cela s'avère indispensable à la fourniture d'un service à la personne concernée. Ainsi concrètement, le transfert de données consécutif à une transaction internationale vers un pays dépourvu d'un niveau de protection adéquat serait autorisé pour autant que la personne concernée y consente. Ce consentement devrait être « informé » au sens où il est entendu dans la proposition de directive, l'information devant être centrée plus spécifiquement sur la non-existence d'un niveau de protection adéquat et le risque dès lors encouru. De plus, les informations ainsi transmises ne devraient pouvoir être utilisées qu'aux seules fins de fourniture du service.

La justification de pareille exception résiderait dans l'intérêt légitime de la personne concernée de décider elle-même de ses besoins personnels. Le transfert se ferait donc dans l'intérêt de la personne concernée souhaitant obtenir un service nécessitant de manière impérative un transfert de données personnelles.

Le consentement comme exception au principe d'interdiction d'exportation vers un pays n'offrant pas de niveau de protection adéquat ne devrait avoir lieu que dans le cadre d'une relation contractuelle ou quasi-contractuelle. Admettre une telle exception rencontrerait les objections de certains commentateurs inquiets de ne pouvoir effectuer des paiements internationaux. Les deux conditions cumulatives, suffisantes à leurs yeux à assurer la protection de l'individu, seraient donc d'une part le consentement informé de la personne concernée au transfert et d'autre part que le transfert ait lieu dans le cadre d'une relation contractuelle et qu'il soit nécessaire pour l'exécution d'une obligation contractuelle.

4. Comités

La proposition de directive institue au niveau européen deux organes distincts chargés de la protection des données, tout en réaffirmant dans le même temps le rôle et l'importance des autorités nationales de protection des données. Il n'en reste pas moins paradoxal de la part de la Commission, en tant qu'auteur du projet, de mettre en place deux nouveaux organismes tout en renforçant parallèlement ses propres compétences. La Commission entend s'octroyer une large part des compétences revenant traditionnellement aux autorités de contrôle nationales.

Examinons de plus près comment se répartissent les prérogatives de chacune de ces institutions.

Qu'adviendra-t-il, dans un premier temps, du rôle des autorités de contrôle telles qu'elles existent dans les différents pays ayant adopté une législation interne de protection des données ? A côté des fonctions et des pouvoirs qui leur sont déjà traditionnellement reconnus, ces autorités se voient chargées d'une mission propre : elles veilleront dans chaque Etat à l'application des dispositions nationales prises en application de la directive. Autorités indépendantes, les autorités de contrôle seront dotées de pouvoirs d'investigation et de contrôle des applications informatiques.

Ensuite, quel sera le rôle dévolu aux deux organes dont la Commission assurera la présidence ?

Le premier, le groupe de protection des données à caractère personnel sera composé de représentants des autorités de contrôle des Etats membres et aura pour mission essentielle de conseiller la Commission sur les questions de protection des données dans la Communauté et dans les pays tiers. Le groupe pourra notamment se prononcer sur le niveau de protection offert par les pays tiers.

Le second, le comité consultatif rassemblera des représentants des Etats membres et interviendra dans le cadre des pouvoirs d'exécution de la Commission.

Enfin, la Commission, si le texte est adopté en l'état actuel, se verra attribuer des compétences supplémentaires.

D'une part, elle disposera d'un pouvoir réglementaire d'exécution en vue d'adapter les dispositions de la directive aux spécificités de certains secteurs. Dans l'exercice de cette compétence, la Commission sera assistée du comité consultatif.

D'autre part, même si la formulation des articles 24 et 25 n'est pas parfaitement claire sur ce point (voir *supra*), c'est à la Commission que reviendra une large part du pouvoir décisionnel en matière de transfert de données à caractère personnel vers des pays tiers. Préalablement à la prise de décision de la Commission, la procédure envisagée prévoit l'intervention obligatoire du comité consultatif mais limite cependant celle-ci à l'émission d'un simple avis. Le choix du comité consultatif au détriment du groupe de la protection des données s'explique sans doute par le fait qu'il s'agit d'une décision politique qui va au-delà des seuls intérêts de la protection des données.

(97) B.W. Napier, « Contractual solutions to the problem of equivalent data protection in transborder data flow, op. cit., p. 33.

(98) Voir A.C.M. Nutger, *Transborder Data Flow of Personal Data within the EEC*, Utrecht, Kluwer, 1990, p. 309.

L'article 25 illustre à souhait le constat du renforcement du pouvoir de la Commission. Il précise que dans l'hypothèse de notification d'opposition, la Commission pourra arrêter les « mesures appropriées ». L'exposé des motifs mentionne à titre d'exemple la possibilité pour la Commission d'interdire le transfert.

La Commission disposera donc d'un pouvoir étendu puisqu'elle pourrait dans ses relations avec les pays tiers, opter pour une politique des flux transfrontières.

Conclusion

Le projet de directive européenne a le mérite d'instaurer un cadre juridique au profit d'une réalité socio-économique qui en était dépourvue. S'adaptant aux évolutions de la société, le droit entend ici remplir sa rassurante fonction : encadrer de règles divers comportements, en l'occurrence ceux liés à la circulation de l'information et des données. Encadrer, tel est effectivement l'objectif de la directive, encadrer un domaine qui par nature postule la mobilité. Encadrer et non encombrer l'information d'une protection excessive. Après l'adoption de la directive, lors de sa transposition dans le droit des Etats membres, il serait bon de garder à l'esprit qu'en la matière protection maximale n'induit pas protection optimale. En effet, trop de protection risque de se ramener à une absence de protection, en raison d'une application trop lourde à réaliser.

Les marges de manœuvre laissées aux Etats membres pour la mise en œuvre de la directive présentent une ambivalence. Assez large, afin de ne pas verser dans un système de protection inflatoire et inhibant, la latitude octroyée aux autorités nationales est peut-être aussi trop large pour espérer atteindre l'harmonisation visée.

La summa divisio opérée dans la directive laisse perplexe. Pourquoi avoir différencié à ce point le régime applicable au secteur public de celui réservé au secteur privé ? L'administration serait-elle davantage à l'abri des dérives informationnelles nuisibles aux individus ?

Enfin, il est permis de se demander si certaines dispositions de la directive résisteront longtemps à l'usure du temps. Le texte actuel sera-t-il à même d'encadrer les nouveautés technologiques d'un secteur en permanente évolution ou bien devra-t-il rapidement être complété et amendé ? Il est vrai qu'on touche ici à un aspect de la finitude du droit. Soumis à l'abstraction et à la généralité, à la poursuite de la réalité sociale explosive, le droit ne la rattrapera jamais tout à fait.

Marie-Hélène BOULANGER
et Cécile de TERWANGNE,
des Facultés Universitaires Notre-Dame de la Paix (Namur),

sous la direction d'Yves POULLET,
Directeur du Centre de Recherche Informatique et Droit (C.R. I.D.).