Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Protection des données à caractère personnel et obligation de sécurité

Poullet, Yves

Published in:
La sécurité informatique, entre technique et droit

Publication date:
1998

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 1998, Protection des données à caractère personnel et obligation de sécurité. dans *La sécurité informatique, entre technique et droit.* Cahiers du CRID, numéro 14, Story Scientia, Bruxelles, pp. 195-224.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. Jul. 2025

B. PROTECTION DES DONNEES A CARACTERE PERSONNEL ET OBLIGATION DE SECURITE

Yves Poullet[29],[30]

1. INTRODUCTION

1. L'obligation d'assurer la sécurité des systèmes d'information constitue une pièce centrale des législations de protection des données à caractère personnel. Elle s'y conçoit dans un double sens : il s'agit tant d'assurer la confidentialité des données, c'est-à-dire le non accès à celles-ci par des personnes non autorisées, mais également leur fiabilité, c'est-à-dire la qualité des données traitées, leur exactitude, leur mise à jour et leur non déformation par le traitement.

Certes, la protection des données ne se réduit pas à leur sécurité. Elle repose sur quatre principes :

— la participation individuelle, qui se conçoit à la fois comme la possibilité pour la personne concernée de connaître (l'accès) voire, dans certains cas, de maîtriser par le consentement ou l'opposition la circulation de son image informationnelle;

— la finalité, qui exige que les raisons pour lesquelles l'information nominative est collectée soient déterminées, explicites et légitimes;

— la proportionnalité, qui s'oppose à ce que le responsable du traitement traite plus de données que celles strictement nécessaires pour l'obtention des finalités;

— la qualité des données, qui s'entend de l'exactitude et de la mise à jour des données.

La sécurité des données n'épuise donc point, loin de là, les exigences posées par ces différents principes. Elle apparaît cependant comme une

---

29 Les présentes réflexions s'inscrivent dans le cadre d'une recherche financée par les S.S.T.C., en particulier pour assurer le soutien à des pôles d'attraction en question regroupe les FUNDP de Namur (CRID et CITA, l'U.L.G. (LENTIC) et la VUB (SMIT) et étudie le devenir et les enjeux de la Société de l'information.

30 Nous tenons à remercier Madame B. Havelange pour l'aide précieuse apportée à l'analyse des risques liés aux traitements de données.

condition *sine qua non* du respect de chacun de ces principes. Sans elle, comment convaincre la personne concernée qui se prévaut de son droit d'accès, que les informations communiquées en conséquence de l'exercice de ce droit soient les seules détenues. Comment affirmer qu'aucune personne non autorisée n'aura jamais accès à des données détenues par le responsable pour des finalités illégitimes ? Comment enfin, garantir la personne concernée contre la non déformation des données voire l'ajout de certaines données non pertinentes ?

2. Ces considérations justifient l'importance des prescrits relatifs à la sécurité des données.

Notre exposé se limitera à quelques réflexions de base tant les applications pourraient varier d'un secteur à l'autre voire d'une technologie à l'autre.

Un premier chapitre identifie les risques et les facteurs de risques dont devra tenir compte tout évaluateur d'un système de sécurité de protection des données qu'il s'agisse du responsable du traitement, d'une société d'audit, de l'autorité de contrôle voire judiciaire.

Le deuxième chapitre analyse les obligations légales de différents intervenants dans le traitement, y compris lors de la communication de données nominatives. Il sera tenu compte à cet égard des prescrits des directives européennes[31] plutôt que de ceux de la loi belge actuelle dont l'adaptation aux dispositions de la directive européenne est de toute façon requise dans les trois ans de la publication.

Enfin, en conclusion, nous soulignerons, à la suite d'un rapport récent[32], comment les exigences déduites des législations de protection des données

---

31 Par directive, nous entendons celle dite générale (Dir. 95/46/CE du Parlement Européen et du Conseil du 24. oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E. n° L 281/31, 23 nov. 1995) et la directive dite Télécommunications 97/66/CE du Parlement européen et le Conseil de l'Union européenne (15/12/97) concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. La terminologie de la présente contribution est fondée sur ces directives et non sur la loi belge du 8 décembre 1992 en instance de révision. Ainsi, on parlera de responsable du traitement et non de maître de fichier, etc.

32 Il s'agit du rapport "Privacy enhancing Technologies. The path to anonymity" - vol. I et II, *Achtergrondstudies en verkenning*, Registratiekamer, The Netherlands & I and P. Commissioner/Ontario, Canada, Aug. 1995.

peuvent militer en faveur de l'utilisation de certaines techniques plus favorables à la protection des données.

CHAPITRE I. RISQUES ET FACTEURS DE RISQUE[33]

A. Définitions : de la notion de dommage à celle de facteur de risque

3. Il importe tout d'abord de distinguer clairement les dommages des risques liés aux traitements de données et secondement de dégager les facteurs susceptibles d'avoir une influence sur ce risque.

a. Notions de "risque" et de "dommage"

4. Le risque est un événement dont la survenance n'est pas certaine mais entraîne pour la personne fichée un dommage.

Dans le cas de traitement de données personnelles, nous avons rangé les risques en quatre grandes catégories, que nous détaillons ci-dessous : ce sont les risques de perte de contrôle, de réutilisation des données, de manque de proportionnalité et d'inexactitude de ces données.

Les dommages, quant à eux, peuvent être d'ordre immatériel, matériel, ou encore concerner la sécurité physique des personnes. Bien que la question de la détermination du type de dommage plus spécifiquement entraîné par la réalisation de l'un ou l'autre des risques identifiés soit examinée en détail ci-dessous, il paraît utile de rappeler brièvement ce que recouvrent ces différentes catégories de dommages.

Le dommage immatériel est une atteinte à la personnalité provenant de la violation d'une liberté ou d'un droit fondamental. Cette violation entraîne par elle-même ce type de dommage, même si il n'y a pas de dommage matériel, ni même moral, au sens classique du terme. Nous préférons le qualificatif d'"immatériel" à celui de "moral" car ce dernier nous paraît répondre à des conditions plus strictes, et ne pas être défini identiquement dans toutes les traditions légales. Pour illustrer cette différence par un

---

33 Ce chapitre s'inspire de réflexions contenues dans un rapport de recherche rédigé à l'attention de la Commission européenne (DG XV) et portant sur la notion de protection adéquate. Ces réflexions ont été rédigées par B. Havelange, A. Lefebvre et Y. Poullet. Un "Executive Summary" rédigé par B. Havelange et Y. Poullet sera publié sous peu par la Commission.

exemple tiré de la matière étudiée, on peut estimer que l'inclusion dans une liste d'adhérents à un parti politique extrémiste constitue un dommage moral, alors que la perte de contrôle sur les données (ne plus savoir qui sait quoi sur soi) représente plutôt un dommage immatériel, même si il n'y a pas de réutilisation de ces données.

Le dommage matériel est le résultat d'une atteinte aux biens d'une personne, ou encore à ses possibilités d'en acquérir, de les accroître ou de les gérer. Il nous semble, par exemple, que la perte d'une chance d'engagement chez un employeur pour des raisons liées à la connaissance par ce dernier d'informations sur la personne constitue un dommage matériel.

L'atteinte à l'intégrité physique est sans doute plus rare dans ce contexte; elle est constituée par les traitements dégradants, les sanctions pénales injustifiées, voire la mort de la personne concernée. Ce type de dommage peut se produire, par exemple, lorsque des données personnelles sont traitées dans un pays soumis à un régime totalitaire susceptible de détourner les données en question.

5. Les trois types de dommages cités ci-dessus peuvent bien entendu apparaître séparément ou simultanément à cause de la réalisation d'un risque. *A priori*, le dommage immatériel paraît le plus bénin, et le dommage "physique" le plus grave, mais il ne nous paraît pas souhaitable d'établir une véritable gradation de ces dommages. En effet, une "échelle" des dommages est toujours sujette à controverses et risque, en outre, de conduire à diminuer la prévention des dommages jugés moins graves. Or, cela ne semble pas entrer dans les intentions du législateur européen, qui vise à protéger les "libertés et droits fondamentaux des personnes"[34], indépendamment du type de dommage éventuellement subi.

b. Notion de "facteur de risques"

On appelle "facteurs de risques" tous les éléments propres à un traitement ou une catégorie de traitements qui sont susceptibles d'avoir une influence sur l'occurrence du risque, soit qu'ils l'augmentent, soit qu'ils la diminuent. Nous reviendrons sur les différents facteurs.

---

34 Article 1 de la Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

B. Description des risques

7. Les risques encourus peuvent être synthétisés comme suit : il s'agit de la perte de contrôle sur les données, de la réutilisation des données par d'autres personnes ou pour d'autres finalités, de la non-conformité des données et de leur inexactitude.

a. Perte de contrôle de la personne fichée sur ses données

8. Le risque visé ici est celui qui consiste, pour la personne fichée, à ne plus savoir "qui sait quoi" sur elle.

De nombreuses dispositions des réglementations de protection des données permettent d'éviter la réalisation de ce risque : l'obligation d'informer la personne concernée, en particulier lorsque les données ne sont point collectées auprès d'elle[35]; l'existence d'un registre public[36] où la fiche d'identité des divers traitements tenus par une entreprise permettra à la personne concernée de prendre connaissance des principales caractéristiques des traitements y opérés; enfin, le droit d'accès qui autorise la personne concernée à prendre connaissance des données traitées la concernant et de la finalité de leurs traitements[37].

9. Notons que la personne fichée ne subit pas nécessairement un dommage *matériel* du fait de cette simple perte de contrôle. S'il ne s'y ajoute ni réutilisation imprévue, ni détournement de finalité, par exemple, le dommage se limite au fait que le citoyen européen est "fiché" en plusieurs endroits sans le savoir.

Par ailleurs, le dommage immatériel peut même dépasser cette simple ignorance sans pour autant devenir quantifiable financièrement. Si, par exemple, une personne achète une arme, et que son nom figure donc sur une liste d'acheteurs, elle pourrait, par suite de recoupements (effectués par des sociétés de marketing) avec certains fichiers, être introduite dans une liste d'amateurs de revues de chasse. Or, bien qu'elle ne subisse pas dans ce cas de dommage matériel, cette personne pouvait légitimement souhaiter

---

35 Il est à noter que les articles 10 et 11 de la directive distinguant précisément de ce fait les règles applicables "en cas de collecte des données auprès de la personne concernée" et celles valables dans les cas de collecte indirecte.

36 C'est le fameux registre "public" tenu par la Commission de protection de la vie privée auquel chaque responsable de traitement, préalablement à la mise en œuvre d'un traitement, sera tenu de notifier les caractéristiques de son traitement (art. 17 de la loi belge, art. 19. 3. de la directive).

37 Il s'agit des articles 10 à 12 de la loi belge, de l'article 12 de la directive.

que ses acquisitions dans ce domaine restent discrètes. Si la personne fichée perd le contrôle sur ses données, elle ne peut demander à être radiée de ces listes.

Enfin, il faut rappeler qu'il est important pour la personne fichée de ne pas perdre la maîtrise sur ses informations, mais qu'en outre, c'est la condition *sine qua non* pour l'exercice d'un contrôle sur les utilisations ultérieures des données, ou encore sur leur exactitude ou leur pertinence. Dès lors, on considère que la perte de contrôle peut non seulement être dommageable en soi, mais qu'elle est susceptible d'entraîner en outre des conséquences en matière de détournement de finalités, ou d'inexactitude des données.

b. Réutilisation des données[38]

10. On considère que la réutilisation des données constitue un risque lorsqu'elle est effectuée à des fins différentes de celles qui étaient annoncées initialement (a), ou encore lorsqu'elle est le fait de personnes non autorisées initialement (b). Notons que ces deux types de réutilisations abusives peuvent facilement se cumuler.

a. En particulier, lorsque les données sont transférées, il existe un grand risque que les données soient réutilisées à d'autres fins que celles prévues initialement. Ce risque peut augmenter selon différents facteurs qui seront développés par après. Ainsi, par exemple, le type de destinataire des données est d'une grande importance : s'il s'agit d'un flux intracorporatif de données du personnel, le risque est moins grand que lorsqu'il s'agit de données envoyées à une firme de marketing.

Le danger évoqué ici est plus concret que celui de la perte de contrôle; en outre, dans la mesure où l'usage abusif a par hypothèse déjà eu lieu, le dommage immatériel de perte de contrôle se double plus souvent d'un dommage matériel.

Les illustrations pratiques du dommage ne manquent pas dans ce domaine. Les systèmes informatisés de réservation aérienne tels Galileo ou Amadeus disposent de codes reprenant telle ou telle caractéristique des passagers empruntant les lignes affiliées. Ces codes concernent aussi bien le statut (VIP, mineur non accompagné) que des caractéristiques telles que "fumeur ou non-fumeur", "diabétique", "repas musulman", etc. Les codes en

---

38 L'article 6 d) de la directive prescrit que les données doivent être "collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées".

question peuvent être transmis aux agences de voyage, ainsi qu'à diverses organisations touristiques travaillant en collaboration avec elles. On imagine sans mal le dommage potentiel si de telles données sont transmises à une compagnie d'assurances, par exemple.

(b) Même s'il n'y a pas de détournement de finalité, la simple utilisation par un tiers non autorisé, pour une finalité éventuellement identique peut constituer un dommage dans certains cas. En effet, si une personne choisit de confier ses données à une organisation ou une firme, c'est en vertu d'une relation existant entre elles, relation qui peut impliquer une certaine confiance. Si les données sont utilisées par d'autres personnes et/ou à d'autres fins, cette relation n'existe plus nécessairement. Par exemple, lorsqu'une personne accepte de confier ses données à une firme de marketing dont elle connaît les pratiques honnêtes et rigoureuses en matière de sécurité, cela ne signifie pas pour autant qu'une autre société, même si elle utilise les données pour une finalité similaire, bénéficiera de la même confiance.

En conclusion, on peut estimer que, si le détournement de finalité constitue un risque si important, c'est essentiellement parce que les causes légitimant le premier traitement peuvent être absentes des traitements ultérieurs.

c. Manque de proportionnalité[39]

11. On parlera de manque de proportionnalité lorsque les données détenues par le responsable du traitement excèdent ce qui est nécessaire pour la réalisation de la finalité annoncée, ou ne sont pas pertinentes par rapport à cette finalité.

Lorsque les données sont croisées par la suite avec d'autres données issues d'autres fichiers, une société pourrait détenir des données superflues pour le traitement prévu, simplement parce qu'elle a acheté un ensemble de données non triées à cet effet.

Le dommage causé dans ce cas est assimilable dans une certaine mesure à la perte de contrôle : les données personnelles étant considérées comme une part de la personnalité de l'individu, il peut légitimement prétendre à ce que le maître du fichier (son employeur, par exemple) ne dispose pas sur lui de plus de renseignements qu'il n'est nécessaire.

---

39 L'article 6 c) de la directive prescrit que les données doivent être "adéquates, pertinentes, et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement".

Un dommage matériel est envisageable aussi car il peut y avoir sur base des données supplémentaires des critères discriminants. Ainsi, on peut trouver, repris dans un contrat de travail, mention de la race de l'employé, ce qui constitue un renseignement non indispensable à l'exécution du contrat, et potentiellement dommageable pour la personne concernée.

d. Utilisation de données inexactes ou obsolètes[40]

12. On envisage ici l'hypothèse où les données détenues sur la personne fichée sont incorrectes et/ou obsolètes.

Il est préjudiciable à la personne concernée que les données traitées relatives à elle-même ne soient pas exactes. En effet, des données inexactes peuvent entraîner la prise de décisions injustes par l'utilisateur des données erronées, ou encore, de manière plus pernicieuse et incontrôlable, l'inclusion sur une liste noire (en matière de crédit ou d'assurance, par exemple). Le dommage causé par ces erreurs peut être extrêmement grave et impossible à corriger par la suite, une fois que les données incorrectes ont été répandues (voire même croisées avec d'autres données).

Ici encore, on peut se trouver face à un dommage moral plutôt que matériel. Ainsi, l'inclusion erronée sur une liste de participants à un meeting d'un parti même non extrémiste peut ne causer aucun dommage matériel mais il est légitime de vouloir corriger cette erreur.

Notons que dans le cas de la réalisation du risque d'inexactitude des données, la personne fichée n'a pas nécessairement perdu totalement le contrôle de ses données : elle peut parfaitement savoir qui les détient et en quel endroit. Par contre, bien qu'elle réalise que les données détenues ne sont par exemple pas exactes, ni mises à jour, la personne concernée peut ne pas parvenir à y accéder. Les barrières psychologiques sont en effet nombreuses vu la relation entre le responsable du traitement et la personne concernée qu'il s'agisse d'obstacles liés à la méconnaissance des institutions et organisations, ou encore de l'impossibilité de se faire aider à établir son droit, …

Cette difficulté d'accès rend problématique la simple connaissance d'erreurs contenues dans les informations, sans parler de leur rectification ou effacement.

---

40 L'art. 6 d) de la directive prescrit que les données doivent être "exactes et, si nécessaires, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées".

C. Les facteurs d'influence

13. On appelle "facteurs d'influence" ou "facteurs de risque" les facteurs propres à un transfert ou une catégorie de transferts et qui sont susceptibles de jouer de différentes manières sur des risques mentionnés plus haut. Le plus souvent, les facteurs d'influence peuvent agir dans les deux sens sur les risques, soit pour les aggraver, soit pour les diminuer.

Certains facteurs sont généraux. Ces facteurs sont propres à diverses caractéristiques de tout traitement : on relève des facteurs liés aux données, à la nature des relations entre la personne concernée et le responsable, aux finalités du traitement et, finalement, aux caractéristiques techniques du système d'information utilisé (i).

Dans le cas où le traitement consiste en la communication à des tiers situés éventuellement à l'étranger, d'autres facteurs s'ajoutent (ii).

a. Facteurs généraux

(1) Facteurs liés aux données

(i) Sensibilité des données

14. On entend par données sensibles[41] au sens de la directive celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et celles relatives à la santé[42] et à la vie sexuelle. Affectent également le

---

41 L'article 8 de la directive définit comme suit la donnée sensible : "Les Etats membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle".

42 La récente Recommandation du Conseil de l'Europe n° R(97)5 adoptée le 13 février 1997 relative à la protection des données médicales décrit largement en son article 9 les mesures de sécurité à prendre et préconise notamment la nomination d'un responsable de données et l'adoption de règlements internes en la matière. Le commentaire de la Recommandation s'exprime à ce sujet comme suit : "Les rédacteurs de la Recommandation ont souligné l'importance croissante des mesures de sécurité, liées à l'utilisation toujours plus grande des équipements électroniques par les praticiens médicaux quels qu'ils soient, les nombreux vols de tels équipements et le coût relativement faible de la mise en place de telles mesures. C'est pourquoi le Principe 9. 2. exige en particulier une politique visant à assurer la sécurité et l'exactitude des systèmes d'information

risque toutes les données dont on peut déduire (éventuellement selon le contexte) de tels éléments[43]. Les données peuvent être sensibles "par nature", au sens de la directive, ou se révéler dangereuses selon le contexte; l'appréciation du caractère sensible des données doit dès lors se faire au cas par cas.

Le caractère sensible ou non des données entraîne des conséquences en matière de proportionnalité des données : si des données sensibles sont réutilisées, on peut être amené à considérer d'office qu'elles sont non proportionnelles, quel que soit le contexte. Par exemple, si des données médicales sont transférées à des fins de recherche, elles seront jugées non proportionnelles pour toute autre utilisation (assurances, marketing, emploi, …). Cela constitue une caractéristique des données sensibles par rapport aux autres : la réutilisation d'une donnée non sensible à de telles fins n'entraîne pas nécessairement un problème de non proportionnalité.

15. Notons que la sensibilité des données agit d'une façon particulière sur l'ensemble des risques. En réalité, elle ne rend pas la réalisation du risque plus probable, mais elle en aggrave les conséquences : si le dommage survient, il est plus grand (la réutilisation de données sensibles, ou leur inexactitude entraînent plus de conséquences dommageables que dans le cas d'autres données).

Ainsi la réutilisation par un employeur potentiel de données relatives à la santé ou aux opinions syndicales d'un employé, données obtenues par hypothèse dans un tout autre contexte, sont susceptibles d'entraîner des

---

médicale y compris par des mesures de protection en matière de sécurité identiques à celles qui ont été définies à l'article 118 de la Convention d'application de l'Accord de Schengen du 14 juin 1985. De telles mesures devraient établir un équilibre entre le fonctionnement souple du système au bénéfice du patient et les garanties nécessaires à la protection de sa vie privée contre toute intrusion inutile. Ces mesures devraient être à la hauteur des développements technologiques des systèmes d'information, sans pour autant donner lieu à des dépenses démesurées".

43 Ainsi, la consultation régulière de pages Web de textes sacrés musulmans permet d'inférer certes, sans certitude complète, l'opinion religieuse du lecteur. On sait que le rapport au Roi de l'Arrêté royal n° 14 du 22 mai 1996 déterminant les fins, les critères et les conditions des traitements autorisés de données visées à l'article 6 de la loi du 8 décembre 1992 tente de distinguer les données qui, selon le contexte, révèlent avec quasi certitude cette opinion et celles qui ne permettent d'inférer cette opinion qu'avec une marge appréciable d'erreur. Ces dernières données ne sont pas dites sensibles.

conséquences discriminatoires (contrôle particulier, refus d'engagement) pour ce dernier.

(ii) Nombre de renseignements

16. On peut penser que plus la masse de données sur une personne est grande, plus le risque est grand. Un risque accru dans ce cas est celui du manque de proportionnalité : plus on dispose de données sur une personne, plus le risque de voir ces données excéder ce qui est strictement nécessaire est élevé.

(iii) Nombre de personnes concernées

17. Le fait de traiter des fichiers concernant un très grand nombre de personnes (par exemple, toute la population d'un pays) aggrave un risque de perte de contrôle sur ces données. En outre, et ceci est valable pour tous les risques, on peut considérer que si un grand nombre de personnes subit un dommage même minime, le risque est plus grand que si peu de personnes subissent ce même dommage.

(2) Facteurs liés aux caractéristiques du responsable du ou des traitements

(i) Nature des relations entre la personne concernée et les responsables des traitements

18. On distinguera ici les traitements issus d'une relation contractuelle ou d'autorité publique entre personne concernée et responsable, de ceux existant en dehors de toute relation de tels types, ainsi en matière de fichiers tenus par des sociétés dites de mailing, des "chasseurs de têtes", des agences de renseignements commerciaux.

La directive reconnaît implicitement pour ces derniers traitements les risques plus importants d'atteinte à la protection des données puisqu'elle exige conformément à l'article 7 f)[44] qu'une balance d'intérêts soit opérée entre, d'une part, l'intérêt de celui qui traite les données, l'intérêt de celui à qui il entend les communiquer (l'employeur potentiel, le prêteur contacté, etc.) et, d'autre part, l'intérêt de la personne concernée.

---

44 L' art. 7 f) légitime le traitement, s'"il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, § 1".

On ajoutera que l'article 14 b) crée un droit d'opposition pour la personne concernée pour toute utilisation de ses données à des fins de démarchage commercial[45].

(ii) Structuration interne du responsable du traitement

19. Il est certain que la multiplication des utilisateurs d'un traitement au sein de l'organisation, leur localisation en des endroits multiples, le cas échéant, accessibles au public entraîne un accroissement des risques de perte de confidentialité des données.

(iii) Mode de collecte des données

20. La collecte directe auprès de l'utilisateur réduit les risques d'inexactitude des données et permet à ce dernier une identification du lieu du ou des traitements de l'information le concernant.

La collecte indirecte, c'est-à-dire auprès d'un tiers, augmente le risque d'inexactitude de données, de perte de contrôle, voire de détournement de finalité.

(3) Facteurs liés aux finalités

(i) Multiplicité et hétérogénéité des finalités

21. La collecte et l'utilisation de données par une entreprise ou une organisation peuvent poursuivre une ou plusieurs finalités, chacune de ces finalités présentant par rapport à l'autre, une plus ou moins grande compatibilité. Ainsi, la banque qui collecte des données peut poursuivre, outre la finalité : "gestion de crédits", celle de démarchage commercial pour des produits de crédit voire pour d'autres produits (assurance, agence de voyages)[46], celle, enfin, de contrôle de la valeur de crédit au regard de l'ensemble des établissements de crédit dans le cadre de la transmission à une banque de données positive de renseignements à propos des crédits à la consommation[47].

---

45 L'art. 14 b) ouvre à la personne concernée "le droit de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection…".

46 C'est le cas FEPRABEL, jugé par le président du tribunal de commerce d'Anvers le 7 juillet 1994 et amplement commenté (*D. C. C. R.* , 1994, p. 77 et s. , note T. Léonard *; Computerrecht*, 1994, p. 244, note J. Dumortier et F. Robben, etc.).

47 A ce propos, lire l'article de T. Léonard, "Fichiers crédits et vie privée : le contexte légal et jurisprudentiel", Conférence donnée à l'Observatoire du

A l'inverse, une entreprise peut collecter une donnée pour une finalité unique et bien déterminée : ainsi, traiter un ordre d'achat en provenance d'un client.

Il est clair que la multiplication des finalités et plus encore l'hétérogénéité des finalités poursuivies par la constitution d'une banque de données unique exigeront, en raison des risques plus grands engendrés, des normes de sécurité plus importantes. Ainsi, pour reprendre l'exemple donné dans notre introduction, une carte patient constitue une banque de données qui peut poursuivre à la fois des finalités administratives, un suivi médical général, un suivi médical spécialisé, bref autant de finalités qui exigent que soient cloisonnés divers traitements et les utilisateurs légitimes de chacun de ces traitements.

(ii) Traitements informatifs et décisionnels

22. Certains traitements ont pour finalité la simple prise d'informations; d'autres sont liés à la prise d'une décision vis-à-vis de la personne concernée. Parmi les traitements de cette seconde catégorie, on distinguera les traitements où la prise de décision constitue la finalité même du traitement[48], ainsi, les systèmes d'évaluation automatique de la valeur du crédit ou de la promotion d'un employé, etc. Il va de soi que la qualité des informations traitées, la délimitation des utilisateurs légitimes des résultats du traitement sont cruciaux pour les traitements de ce dernier type alors que des traitements constituant une simple prise d'informations représentent des risques moins importants[49] : ainsi, une bibliothèque offrant l'accès à des banques de données bibliographiques.

---

crédit à la consommation, 1996, 30 pages, à paraître; Y. Poullet, A. Lefebvre, "Vie privée et crédit à la consommation, protéger le consommateur ou la vie privée : un choix difficile", in *Le crédit à la consommation*, Bruxelles, Ed. Jeune Barreau de Bruxelles, 1997, p..

48 L'article 15 de la directive générale leur accorde d'ailleurs une importance particulière en reconnaissant à toute personne "le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destinées à évaluer certains aspects de sa personnalité…".

49 Ceci n'exclut pas que d'autres facteurs de risques, par ex. la sensibilité des données en cause, peuvent conduire à la prise de mesures de sécurité comparables.

(4) Facteurs liés aux caractéristiques techniques du système d'information du responsable du traitement

23. La technologie utilisée pour le ou les traitement(s) influence bien évidemment le risque encouru : les informations collectées et traitées par des ordinateurs personnels non interconnectés ou connectés uniquement sur base de la décision de l'utilisateur légitime du système d'information local peuvent à première vue présenter moins de risque que des systèmes largement intégrés et centralisés auxquels chaque utilisateur peut accéder.

Le système full-text présente également plus de danger que des systèmes de base de données relationnelles, renvoyant le cas échéant à des dossiers individuels tenus en dehors du système géré électroniquement.

On ajoute que le système des hyperliens permet des recoupements de données au départ localisés dans des endroits bien différents[50].

Enfin, l'utilisation de numéros d'identification communs à divers traitements[51] facilite des accès illégitimes d'un traitement à un autre, même si, à l'inverse, il évite des erreurs par l'attribution à une personne de données concernant une autre personne.

b. Facteurs spécifiques liés à la communication de données à des tiers

24. La transmission de données peut s'opérer tantôt vis-à-vis de destinataires soumis aux responsables du traitement, tantôt vis-à-vis de tiers. La directive distingue ainsi les transmissions internes au sein de l'organisation d'un responsable de traitement[52] et celles externes vers des tiers, c'est-à-dire "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le

---

50 … dans ce cas, on considère, selon la directive, que cet ensemble logique et non physique de données constitue un seul et même traitement, au sens de l'article 2 de cette directive.

51 Ainsi, le numéro de sécurité sociale ou le numéro de registre national dont on comprend dès lors que l'utilisation soit sévèrement contrôlée et réglementée. A ce propos, l'article 8. 7 de la directive prescrit que "les Etats membres déterminent les conditions dans lesquelles un numéro d'identification ou tout autre identifiant de portée générale, peut faire l'objet d'un traitement".

52 Cf. à ce propos, la définition de la notion de "responsable de traitement" donnée par l'article 2 f) de la directive. Par "responsable du traitement", on entend la personne physique ou morale ou l'association de fait qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel".

responsable du traitement et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données"[53].

Une telle distinction constitue la reconnaissance implicite du fait que la communication externe représente des risques supplémentaires du fait que la personne concernée peut à cette occasion perdre le contrôle de ses données, n'a plus les garanties nécessaires quant au respect par le tiers des finalités préalablement annoncées et de ce fait ne peut être certain que soit encore assuré le respect du principe de proportionnalité.

On distinguera différents facteurs de risques, selon les caractéristiques du flux (***1***), suivant les relations existantes entre l'acteur émetteur des données et l'acteur récepteur des données (***2***), suivant les finalités poursuivies par l'un et l'autre de ces acteurs (***3***). Enfin, d'autres facteurs s'ajouteront lorsqu'il s'agit de transferts internationaux. Nous ne pourrons les envisager dans le cadre de cette brève introduction[54].

(1) Critères liés aux caractéristiques du flux lui-même

(i) Fréquence des flux

25. On peut estimer que la fréquence des flux diminue les risques, dans la mesure où une société qui a l'habitude de recevoir une grande quantité de données adaptera ses structures et sera sans doute mieux organisée qu'une société qui ne reçoit des fichiers qu'occasionnellement. Par exemple, la société peut mettre en place une personne uniquement chargée de traiter les flux alors qu'en cas de flux occasionnels, l'organisation peut être moins bonne.

Le risque concerné peut être la réutilisation des données, éventuellement par une personne non autorisée profitant du manque d'organisation pour intercepter les informations.

Notons que des flux fréquents peuvent diminuer le risque d'inexactitude, dans la mesure où ils favorisent une mise à jour plus fréquente. Cela ne

---

53 C'est ainsi qu'est définie la notion de tiers à l'article 2 de la directive.

54 L'étude précitée remise à la Commission européenne les énumère comme suit : a) la situation politique du pays tiers, b) l'état de la technologie, auquel elle ajoute le critère plus flou de la "différence culturelle". Cette différence culturelle peut provenir de l'appréhension que le pays tiers a des enjeux de la protection des données, de la "corporate culture" de ce pays, des pratiques commerciales, de sa considération quant au caractère sensible des données.

vaut naturellement que pour des flux récurrents portant sur les mêmes types de données.

(ii) Type de transfert

26. Les données peuvent être communiquées par différents types de réseaux :

- Les fichiers peuvent être envoyés par réseau privé. Dans beaucoup de cas, les sociétés importantes louent une ligne privée aux opérateurs de télécommunications afin de relier leurs différentes implantations. Une société mère peut être reliée à ses filiales à travers le monde. Les informations transitent par ce réseau fermé sans gros risques, à condition bien sûr que des mesures de sécurité soient bien établies.

- En revanche, si les données sont envoyées *via* Internet, elles transitent par un réseau ouvert beaucoup plus dangereux. Plus particulièrement, la réutilisation est quasi inévitable dès que les données figurent sur un site Web. La personne concernée perd alors immanquablement le contrôle sur ses données, à moins de les protéger (cryptage); car des réutilisations sont possibles par tous et en tout lieu.

Le risque accru par les possibilités d'interception de ces données sur un réseau ouvert et/ou mal protégé est celui de la perte de contrôle et de la réutilisation des données.

Les données peuvent également être transférées sur des supports plus traditionnels : papier, cassettes, disquettes, etc. Il convient alors d'être attentif au risque d'interception de ce genre de supports. Même dans un pays où la technologie n'est pas fort avancée, le détournement ou la copie clandestine d'une liste de données imprimées peuvent être relativement aisés.

(2) Critères liés aux relations entre acteurs

(i) Liens économiques, légaux, sociaux ou professionnels entre les différents acteurs

27. Si le flux s'intègre dans une relation commerciale ou professionnelle plus générale ou dans des relations entre une société mère et ses filiales, le risque de perte de contrôle est moindre car il y a moyen de retrouver la trace des données auprès du premier responsable. En outre, les finalités sont souvent liées (par exemple, gestion de groupes de donneurs d'organes pour les hôpitaux; gestion du personnel ou de la clientèle pour une société et ses filiales, …), ce qui diminue également le risque. Cela étant, on ne peut négliger le fait que, vu la diversification des activités de sociétés importantes dans des secteurs parfois fort divers (électronique, audiovisuel, presse, divertissement), le risque de réutilisation des données personnelles au sein du groupe ait lieu pour des finalités différentes.

(ii) Secteur d'activité du destinataire

28. Le secteur d'activité du destinataire, en particulier lorsque celui-ci est une société de marketing, est susceptible d'entraîner une aggravation de certains risques, essentiellement en raison de l'utilisation prévisible des données par ce dernier. Dans ce secteur, la réutilisation des données, leur commercialisation, leur croisement avec d'autres fichiers sont en effet systématiques car ces activités sont essentielles au secteur en question. On pense aux sociétés de renseignements en matière d'octroi de crédit, ou encore aux sociétés de courtage de données à caractère personnel, qui amplifient encore le risque car, dans leur cas, la réutilisation est systématique et n'est pas nécessairement limitée au secteur d'origine des données.

Les risques accrus sont essentiellement ceux de la perte de contrôle et de la réutilisation.

(3) Critères liés à la finalité

(i) Cohérence dans les finalités

29. Si les traitements sont indépendants les uns des autres (par exemple, une multinationale vendant certaines données relatives à son personnel à une société commerciale qui les utilisera pour faire la promotion de ses propres produits), le risque est plus grand que si le flux peut être analysé comme une étape d'un processus plus général (par exemple, différentes filiales d'une multinationale s'échangeant des données sur leur personnel pour leurs besoins internes ou agence de voyage transmettant des données relatives à un voyageur à une compagnie d'aviation, à un hôtel, …).

Le risque de perte de contrôle et de réutilisation avec détournement de finalité diminue en effet lorsque l'ensemble des transferts et traitements participent d'une finalité unique : gestion du personnel, organisation de voyages, par exemple.

(ii) Durée de conservation des données

30. La durée de conservation des données pose des problèmes en termes de finalité : le plus souvent, les données sont traitées pour une finalité et conservées pour une finalité liée à la première (à fins de preuve, par exemple). Or, si les données peuvent être nécessaires pendant un certain temps à la réalisation d'une finalité, leur archivage complet peut excéder ces finalités.

C'est donc principalement un risque de non proportionnalité qui se pose, lorsque la durée du traitement est illimitée : des données adéquates et non excessives pour la réalisation d'une finalité de gestion du personnel, peuvent être légèrement excessives pour un archivage à fins de preuve, et

totalement non proportionnelles lorsque cet archivage ne se justifie plus raisonnablement.

En outre, le risque de réutilisation peut également se trouver augmenté. Ainsi, en matière de rencontres sportives (jeux olympiques, par exemple), il peut y avoir des flux de données nominatives à travers le monde pendant un laps de temps limité. Les renseignements concernant les dossiers des athlètes sont envoyés à l'instance organisatrice par les fédérations nationales avant les jeux et le dossier de chaque athlète mentionne le nom, la discipline mais aussi le poids, la taille et éventuellement les résultats de tests antidopage. La finalité de ces flux est claire puisqu'il s'agit d'organiser les rencontres sportives mais ces fichiers restent dans les ordinateurs et peuvent servir plusieurs années après pour d'autres finalités.

Notons enfin que le risque d'inexactitude des données augmente corollairement à la durée de traitement, surtout lorsque le flux a été exceptionnel et n'est pas mis à jour régulièrement.

(iii) Finalité déterminée ou non

31. Il peut arriver que la finalité du transfert soit mal ou pas définie, mais il nous semble qu'une détermination insuffisante des finalités soit plutôt à craindre dans le contexte de certains transferts par Internet : c'est le cas lorsqu'on laisse ses coordonnées dans un "livre d'or" proposé sur un site Web. Les personnes qui ont parcouru les informations sont simplement invitées à laisser leurs coordonnées et éventuellement une appréciation : la finalité n'est pas définie.

Cela étant, même hors du contexte des transferts par Internet, il est imaginable que la finalité d'un transfert soit suffisamment définie pour être en conformité avec le prescrit de la directive en la matière, mais que ce premier transfert puisse en générer d'autres moins bien contrôlés et définis.

c. Evaluation des risques

32. La description des divers facteurs permettra au responsable du traitement l'évaluation des risques encourus en matière de protection des données. Certains facteurs peuvent jouer de manière positive, d'autres, de manière négative. Certains facteurs peuvent être ambivalents : constituer un facteur aggravant au regard du risque dit de manque de proportionnalité mais, au contraire, un facteur de diminution du risque d'inexactitude de données. On l'a noté, par exemple, à propos de l'utilisation de numéro d'identification. L'absence de relations économiques, légales, sociales ou professionnelles entre l'émetteur d'un flux et le destinataire suscite *a priori* la crainte d'un risque de réutilisation de données, illégitime dans le chef du

destinataire, mais amène certainement l'émetteur à limiter plus étroitement les données transmises à ce destinataire non naturel.

Le responsable du traitement est donc invité au regard du traitement concerné à évaluer la présence de chaque facteur de risque et à en mesurer de manière raisonnable la portée pour chacun des risques identifiés. Ainsi, il pourra déterminer le ou les risques majeurs : s'agit-il d'un risque de réutilisation des données, de manque de proportionnalité, d'absence de qualité des données, de perte de contrôle ? Les réponses adéquates varieront selon la nature du ou des risques ainsi identifiés. Ainsi, un système expert d'aide au diagnostic médical pour un médecin travaillant avec un ordinateur personnel non connecté soulève essentiellement le risque d'inexactitude de données; le même système expert dans un hôpital fonctionnant en réseau ouvert avec des médecins de la région ajoutera d'autres risques au premier, à savoir la réutilisation illégitime et l'absence de proportionnalité.

La prise en compte d'autres facteurs de risque justifiera alors d'autres mesures.

33. Un rapport de la Registratiekamer des Pays Bas[55] suggère qu'au terme de l'analyse des facteurs de risques, le responsable du traitement détermine, suivant le degré de(s) risque(s) encourus, la classe à laquelle appartient son traitement. Il suggère trois "exclusiviteitsklassen".

- le niveau *de base* qui exigera le "paquet" de mesures dites de base

- le niveau de risque *aggravé* qui nécessitera quelques mesures supplémentaires

- le *haut* niveau de risque qui conduit à la prise de mesures exceptionnelles.

Même si cette approche apparaît quelque peu sommaire au regard d'une analyse qui exigerait, selon les explications ci-dessus, une meilleure distinction des risques et une appréciation plus fine de chaque facteur et de leur combinaison, elle s'inscrit dans une perspective comparable à la nôtre.

---

55 Beveiling van persoonsregistratie, Nov. 1994, Uitgrave Registratiekamer, ISBN 9034631230, disponible auprès de l'éditeur (Postbus 3011-2280 6A Rijkswijk NL).

CHAPITRE II. LES OBLIGATIONS LEGALES DE SECURITE CONSACREES PAR LES LEGISLATIONS DE PROTECTION DES DONNEES

34. Les articles 16 et 17 de la directive européenne dite directive "générale" fixent des obligations légales à charge de divers acteurs. On y ajoutera quelques dispositions de la directive "télécommunications" à propos du transporteur et des divers opérateurs de services de télécommunications soumis à cette directive dite "télécommunications"[56].

A. Les obligations du responsable du traitement[57]

Le premier acteur visé est certes le responsable du traitement.

L'article 17 alinéa 1 de la directive stipule que "le responsable du traitement doit…

a. La notion de responsable

35. Que faut-il entendre par "responsable du traitement"[58], l'article 1 d) de la directive le définit comme suit :

Qu'il soit clair que la notion de responsable vise l'instance responsable de la définition des finalités et des moyens du traitement[59] et non la personne physique en charge de l'exécution des décisions. Ainsi, le responsable sera, non le directeur d'un centre de traitement de l'information ni le chef de la

---

56 Directive 97/66/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications à la note **(1)**

57 Pour rappel, nous avons délibérément opté pour la terminologie européenne.

58 La loi belge parle de "maître de fichier" qu'elle définit comme "la personne physique ou morale ou l'association de fait compétente pour décider de la finalité du traitement ou des catégories de données devant y figurer". Le "ou" pose difficulté lorsqu'on imagine comme possible que l'instance qui définit les finalités des traitements ne soit pas en même temps celle qui définit un moyen d'obtention de ces finalités, à savoir les "catégories de données" à traiter.

59 La version anglaise de la directive utilise à bon escient le mot "controller".

sécurité, mais le plus souvent la personne morale elle-même incarnée par son conseil d'Administration. La définition de la directive a un double sens : elle est à la fois de l'ordre de la constatation, lorsqu'elle se réfère à l'instance qui décide des finalités et moyens des traitements, et de l'ordre de la disposition, puisqu'elle exige qu'une même instance définisse clairement finalités et moyens des traitements.

La suite de la directive place sur les épaules du responsable de lourdes charges dans la mesure où lui incombent à la fois l'obligation d'information de la personne concernée (art. 10 et s.), l'obligation d'assurer la conformité des traitements aux requis de qualité et de légitimité des traitements (art. 6 et s.), et enfin l'obligation de sécurité que nous allons développer ci-après.

b. Les mesures de sécurité[60]

36. Parmi les "moyens" à définir par le responsable du traitement, figurent les mesures de sécurité techniques et organisationnelles "appropriées". La loi belge[61] actuelle contient à ce propos des précisions. L'article 16 § 12 de la loi parle de la conformité des programmes; l'article 16 § 2 envisage une mesure organisationnelle particulière : "l'information des employés, et en général de toute personne ayant accès aux données, à propos des dispositions de la loi et des autres dispositions pertinentes destinées à la protection des données à caractère personnel"[62].

37. L'étude récente de la "Registratiekamer" néerlandaise "Beveiling van persoonsregistraties"[63], déjà citée, détaillait comme suit les grandes catégories de mesures organisationnelles et techniques.

---

60 A ce propos, voy. les dispositions très détaillées de la loi autrichienne (§ 10, BDSG du 18 août 1978, B.G. Blatt n° 565/1978).

61 Pour une analyse des dispositions de la loi, lire A. Pipers, *Le respect de la vie privée*, Ed. Politeia, 1995, p. 142 et s.

62 Ainsi, pour le personnel bancaire affecté aux opérations de crédit, on songera à la loi du 12 juin 1991 relative au crédit à la consommation et à la recommandation du Conseil de l'Europe R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (exemple donné par le rapport Merckx-Van Goey).

Autre exemple, les fonctionnaires communaux habilités à accéder au Registre National doivent être informés des dispositions de la loi du 8 août 1983 organisant un Registre national des personnes physiques.

63 Document établi en nov. 1994 (ISBN 90 346 31230) disponible auprès de la Registratiekamer (PB 3011 2280 GA Rijskwijk). Nous avons

(1) Gestion (Beleid) et organisation de la sécurité

La formulation d'un projet "gestion de la sécurité de l'information" est un requis. Suivra logiquement, la définition d'un plan et de mesures de sécurité. Chaque travailleur de l'organisation devra être conscient de l'existence de ces règles et des conséquences du non respect de celles-ci.

(2) Système et software de sécurité

Les spécifications des systèmes et logiciels de traitement de l'information doivent tenir compte des exigences de sécurité.

(3) Documentation

On retrouve ici l'idée de "l'état" des traitements visé par l'article 16 § 1 de la loi belge et rendu obligatoire par lui, c'est-à-dire de la consignation, pour chaque traitement, de la nature des données traitées, du but du traitement, des utilisateurs des traitements et des interconnexions entre fichiers.

(4) Conception et confection des instruments porteurs de données (gegevensdragers) (disquettes, bandes magnétiques, CD Rom)

Leurs utilisation et conservation doivent être conçues de manière telle que seules les personnes autorisées puissent disposer de leur contenu partiellement ou totalement.

(5) Profils de sécurité

Il s'agit de définir les catégories d'utilisateurs suivant leur autorisation d'accès aux données. Cette définition doit servir à la programmation et aux techniques ou organes de contrôle. Ces autorisations peuvent être temporaires ou définitives, fixées ou non par écrit. Chaque titulaire d'une autorisation doit s'engager à respecter les conditions de son autorisation et souscrire un engagement de confidentialité.

---

regroupé les 14 mesures détaillées par le rapport en 12 mesures. Chaque mesure est décrite dans le rapport selon les 3 niveaux de risque dégagés par les chapitres précédents et évoqués en conclusion du point 2 ci-avant.

On se référera également à l'ouvrage fort complet et très pratique publié en 1987 par The chartered Institute of public finance and accountancy, C. POUNDER, M. KOSTEN, S. PAPADOPOULOS, A. RICHARD, *Managing Data Protection*, CIPFA, London, 1987.

(6) Formation des employés

(7) Registre des flux d'entrée et de sortie

Il est important de veiller à ce que les flux d'entrée proviennent de sources autorisées et que les flux de sortie aboutissent aux personnes autorisées et dans la mesure autorisée.

(8) Organisation administrative

L'organisation administrative de l'entreprise doit être conforme aux impératifs de sécurité[64]. Il serait malsain que les circuits administratifs du responsable du traitement exigent une circulation des données non en accord avec les règles de protection des données; ainsi une direction financière n'a point à connaître des données relatives aux communications d'un employé mais bien de la facture globale liée à de telles communications.

(9) Elimination des traitements ou données superflus

L'analyse des flux et traitement opérés au sein de l'entreprise peut amener le responsable des traitements à déceler des traitements, fichiers ou données redondants, superflus ou non à jour. Il procédera alors, le cas échéant, à l'élimination de ces traitements, fichiers ou données. On ajoutera que c'est un des grands mérites des réglementations de protection des données, par l'exigence qu'elles imposent aux organisations d'analyser leurs systèmes d'information, d'avoir contribué à un nettoyage interne des fichiers et ainsi à une réduction des frais liés à leur traitement ou leur maintenance.

(10) Utilisation de périphériques et d'écrans. Contrôle d'accès et authentification des utilisations

Il s'agit ici de prendre en considération les risques d'accès non autorisé que représentent de tels éléments d'un système d'information. Les contrôles d'accès, des règles relatives à la fermeture des postes, à l'extinction des écrans sont nécessaires. L'enregistrement des accès, voire l'obligation de signature des modifications ou inscriptions de données, peuvent être requis.

(11) Traitement des données

Des procédures de vérification de la qualité des données et des programmes utilisés doivent être implantées, en particulier lorsque les traitements

---

64 A ce propos, par exemple, les "Advices to Management on the disclosure of personal data", publiés en annexe 6 de l'ouvrage de C. POUNDER, M. KOSTEN, S. PAPADOPOULOS, A. RICHARD, *Managing Data Protection*, CIPFA, London, 1987, 321 et s.

portent pour chaque personne concernée sur des quantités importantes de données ou que celles-ci s'avèrent sensibles.

***(12) Convention avec les employés*[65]**

Des engagements spécifiques doivent être exigés tant à propos de la confidentialité des informations auxquelles les employés ont accès qu'à propos de leur respect des mesures de sécurité. Des mesures, tel le renvoi pour motif grave, doivent sanctionner la non exécution de ces engagements.

c. A propos d'une mesure de sécurité particulière : la désignation d'un "détaché à la protection des données"

Parmi les mesures susceptibles d'être prévues par le responsable du traitement, figure la désignation d'un "détaché à la protection des données". Cette mesure de sécurité est particulière dans la mesure où elle constitue une garantie organisationnelle particulière de protection des données mais en même temps garantit l'effectivité des autres mesures de sécurité. Le § 36, alinéa 1 de la loi allemande rend obligatoire cette nomination pour toute administration et entreprise ayant une certaine dimension.

La tâche de ce "détaché" (le Bundesdatenschutzbeauftragte) est multiple[66]. Il veille au respect, par l'organisation qui l'emploie, des réglementations de

---

65 A ce propos, les § 20 al. 2, 3, 4 et 5 de la BDSG (Bundesdatenschutzsgesetz) autrichienne :

"**(2)** Data controllers and service processors shall conclude contracts with their employees, where those explicity stipulate the transmission of automatically processed data only on the basis of instructions according to p. 1 and keep the data confidential even after the end of the contractual relationship to the data controller or service processor.

(3) The empoyer shall be responsable for the completeness and the lawfulness of instructions concerning transmission of data and for providing sufficient information to the employees about these instructions.

(4) The refusal of an employee to carry out an information infringing sec. 18. may not lead to any detriment of the employee.

(5) Nobody is entitled to invoke the confidentiality of data as a reason for withholding testimony in official proceedings".

66 Les §§ 36 et 37 de la loi allemande détaillent à la fois le statut et les fonctions de ce préposé à la protection des données. Sur ces dispositions,

protection des données, diffuse l'information sur les développements nouveaux en matière de protection des données, tient un état des traitements du responsable des données. Il interviendra dans la nomination de personnes en charge des opérations portant sur des données nominatives et dans les demandes d'accès adressées au responsable du traitement.

Dépendant directement de la direction de l'organisation responsable du traitement, il est statutairement indépendant dans l'exercice de ses fonctions et sa révocation est soumise à des conditions strictes. En cas de doute sur la correcte application de la réglementation de protection des données, il s'adressera à l'autorité de contrôle. Enfin, des réunions entre "Bundesdatenschutzbeauftragten" permettent à ceux-ci de développer des actions communes[67].

39. Le modèle allemand a été repris en Belgique dans le domaine de la sécurité sociale. L'article 24 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de sécurité sociale[68] prévoit la nomination par chaque institution de sécurité sociale d'un administrateur responsable de ses banques de données de sécurité sociale et, sur avis conforme du comité de surveillance, d'un responsable informatique chargé de l'organisation des échanges de données. Ils ont pour tâche, selon l'article 25 de la loi, de veiller à "ce que les programmes de traitement ou d'échange automatisé soient exclusivement conçus et utilisés conformément à la présente loi et à ses mesures d'exécution" (art. 25).

On ajoutera la création par l'article 54 de la même loi d'un corps d'inspecteurs sociaux qui contrôleront l'application de la loi et, dans ce cadre, pourront requérir l'assistance de la force publique, donneront des avertissements et fixeront des délais pour l'observation des règles légales. Ils ne peuvent être chargés d'autres missions dans l'institution dont ils relèvent administrativement".

---

on se référera notamment aux commentaires de Tinnefeld et Ehmann, *Einführung in das Datenschutzrecht*, 2e éd. , Oldenburg, 1994, p. 226 et s.

67 Les "détachés à la protection des données" des Länder et de l'Etat fédéral tiennent chaque année une "convention" dont peuvent émaner des décisions. Ainsi, la décision (Beschluss) de la réunion tenue les 27/28 avril 1988, affirme le devoir du responsable de traitement de pourvoir au soutien matériel et en personnel du détaché et ce à charge de l'organisme dont ils dépendent.

68 Loi du 15 janvier 1990, *M. B*., 22 février 1990.

Au-delà de ce secteur spécifique, certaines entreprises[69] n'ont pas hésité à l'adopter spontanément. Sans doute, faut-il regretter qu'aucune disposition réglementaire ne vienne garantir leur indépendance et que, dès lors, on puisse craindre le caractère délicat de leur position lorsqu'il s'agira pour eux d'intervenir contre les intérêts de l'entreprise en faveur de la protection des données.

40. La directive européenne contient une disposition favorisant l'adoption d'une telle mesure : l'article 18. 2 permet aux Etats membres de dispenser[70] les responsables des traitements de toute notification à l'autorité de contrôle "lorsque le responsable du traitement désigne conformément au droit national auquel il est soumis un détaché à la protection des données…".[71]

On notera que la directive renvoie à des dispositions de droit national pour la création d'une telle possibilité. Ces dispositions devraient définir le statut des détachés et leur garantir l'indépendance d'action réclamée par la directive. On regrettera qu'aucune précision n'ait été apportée en ce sens dans le projet de loi modifiant notre loi de protection de la vie privée et actuellement en discussion au sein du gouvernement.

d. Les mesures de sécurité "adéquates"

41. "Les mesures doivent assurer un niveau de protection adéquate." Plusieurs critères sont énoncés par la directive ou par la loi belge[72]à propos de l'appréciation du caractère adéquat :

- l'état de l'art en matière de techniques de sécurité (a);

- les frais qu'entraîne l'application des mesures (b);

---

69 Ainsi, en particulier, chez nous, les organismes bancaires et les établissements hospitaliers.

70 ou de simplifier l'obligation de notification. Il est à noter qu'en Allemagne, dans le secteur privé, aucune notification n'est prévue à charge du responsable du traitement dans la mesure où, d'une part, l'institution du détaché permet un contrôle interne, ce qui permet d'alléger le contrôle externe de l'autorité de contrôle et d'autre part, le détaché a pour tâche de tenir un état des traitements accessible à première demande par l'autorité de contrôle.

71 Ce détaché aura notamment pour mission d'assurer l'application interne des dispositions de protection des données et de tenir un registre des traitements effectués par le responsable du traitement.

72 L'article 16 de la loi belge du 8 décembre 1992 ne s'écarte pas du texte européen.

- la nature des données à protéger (c);
- les risques potentiels d'atteinte à la sécurité des transactions (d).

A Pipers[73] propose une certaine démarche fondée sur une approche chronologique des critères. La nature sensible des données apparaît, selon cette approche, comme le premier critère à prendre en considération avant d'évaluer les risques. Le chapitre I propose divers critères pour l'évaluation de facteurs de risque. Parmi ces facteurs figure la nature des données. Nous y renvoyons le lecteur.

La référence légale à l'état de la technique oblige le responsable du traitement à s'informer des diverses techniques de sécurité présentes sur le marché et à les évaluer à l'aune des risques décelés. Ainsi, on ne traitera pas de la même manière les risques internes à une entreprise vis-à-vis des employés et les risques externes lors de la communication à des tiers.

On insiste sur le fait que ces techniques doivent être présentes sur le marché comme produits déjà commercialisés et non encore à l'état de prototypes et donc difficilement disponibles.

Enfin, l'évaluation des frais ne peut se concevoir en fonction des ressources financières du responsable du traitement. Les frais doivent être suffisants et raisonnables compte tenu des précédents critères. Il serait inacceptable qu'un responsable des traitements limite la sécurité de son système d'information nonobstant les risques encourus pour les personnes concernées au seul motif que les techniques disponibles sont trop onéreuses au regard de ses ressources financières.

Toutes ces mesures n'apporteront sans doute pas la sécurité totale du système. L'exposé des motifs met à charge du responsable non une obligation de résultat mais une obligation de moyens, c'est-à-dire prendre les mesures que prendrait un responsable de traitements[74] diligent au vu des critères énumérés afin d'assurer la protection des données des personnes

---

73 A. Pipers, *Le respect de la vie privée*, Bruxelles, Ed. Politeia, 1995, p. 147 et s.

74 " L'article 17 énumère les obligations qui incombent au maître du fichier d'un traitement de données à caractère personnel. Cette disposition instaure un véritable contrôle interne du traitement. Comme dans le cadre de l'article 13, les obligations doivent s'entendre de façon raisonnable. On se situe d'ailleurs pour l'essentiel dans le cadre d'obligations de moyens et ne seront nécessaires que les mesures dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent ". (Exposé des motifs, projet de loi relatif à la Protection de la vie privée à l'égard des traitements de données à caractère personnel, Ch. des Représ., Sess. 1990-1991, 6 mai 1991, 1610-1-90-91).

concernées. Lorsqu'un dommage survient et révèle un manque de sécurité, ce sera donc à ces dernières de démontrer que ce manque était inacceptable au regard du critère du responsable diligent.

B. Les obligations des employés et sous-traitants

L'article 16 de la directive prescrit à toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant ainsi qu'au sous-traitant lui-même, qui accède à des données à caractère personnel, de ne les traiter que sur instruction du responsable du traitement sauf, ajoute le texte, en vertu d'obligations légales.

La loi belge ne contient pas de disposition de ce type héritée de législations étrangères. Ainsi, la loi autrichienne prescrit en sa section 20 :

La comparaison des textes autrichien et européen permet de comprendre la portée de cette obligation dite de confidentialité. Premièrement, on notera que cette obligation vise tant le responsable du traitement que l'employé ou le sous traitant. Au premier, il est donné ordre de prévoir des "instructions" et cela dans le cadre de contrats écrits stipulant expressément les limites des compétences des seconds et prévoyant une obligation de confidentialité y compris au-delà du terme des relations contractuelles qui les lient. La loi autrichienne ajoute qu'il incombe au responsable de prévoir une information suffisante des employés à propos de ces instructions[75].

Aux employés, la loi autrichienne impose le devoir de respecter de telles instructions. La loi autrichienne limite cette obligation aux traitements automatisés, limite que la directive ne reprend pas. Cette même loi éclaire l'expression sibylline "sauf en vertu d'obligations légales"[76] lorsqu'elle affirme que le devoir de confidentialité ne peut justifier le refus de témoigner en justice. On ajoutera l'intérêt de la disposition autrichienne qui considère que le refus de l'employé de suivre une instruction du

---

75 On notera toutefois l'article 27 de la loi du 15 janvier 1990 (M. B. 22 févr. 1990) qui prescrit l'obligation pour "toute personne qui occupe du personnel et qui a enregistré des données sociales à caractère personnel ou à qui de telles données ont été communiquées" d'afficher, à un endroit apparent et accessible, un avis indiquant où, dans l'entreprise, le texte de la présente loi et de ses arrêtés d'exécution peut être consulté". Tout travailleur doit pouvoir en prendre connaissance "en permanence", "sans intermédiaire" et dans un lieu "aisément accessible" (art. 27).

76 Cf. dans le même sens, l'article 28 de la loi du 15 janvier 1990 (citée note précédente).

responsable contraire aux principes de la protection des données ne peut porter préjudice à cet employé.

L'article 17 de la directive prescrit des devoirs supplémentaires pour le responsable du traitement qui recourt à un "sous-traitant" (le "processor")[77]. Ainsi, seuls peuvent être retenus les "sous-traitants" qui apportent des "garanties suffisantes", notion à apprécier suivant les traitements à mettre en œuvre[78] et les risques y liés.

Le responsable aura soin en outre de rédiger avec le sous-traitant un contrat écrit[79] contenant entre autres comme stipulations, le devoir du sous-traitant de n'agir que sur instruction du responsable et la mise à charge du sous-traitant des obligations de sécurité prévues au § 1 de l'article 17 (mesures techniques et d'organisation appropriées) et, le cas échéant, précisées par la législation de l'Etat membre dans lequel le sous-traitant est établi[80].

C. Les obligations des prestataires de services de télécommunications accessibles au public

44. La directive en voie d'adoption relative "au traitement de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications", directive dite "télécoms", prescrit certaines obligations de sécurité particulières pour les prestataires de services de télécommunications accessibles au public[81]**,** ainsi les prestataires de services de certification, de courrier électronique, les sociétés offrant un

---

77 L'article 2 c) de la directive définit comme suit le "sous-traitant" : "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement".

78 Ce prescrit pourrait conduire à exiger du sous-traitant l'obtention d'un certificat délivré par une société d'audit.

79 ou "sous une autre forme équivalente" selon l'article 4, et ce selon l'exposé des motifs de la directive, pour des raisons de conservation des preuves.

80 On s'interroge : ceci signifie-t-il que le sous-traitant doit nécessairement être établi sur le territoire de l'Union européenne ?

81 La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de télécommunications accessibles au public, sur les réseaux publics de télécommunications dans la Communauté, notamment *via* le réseau numérique à intégration de services (RNIS) et les réseaux numériques mobiles publics (art. 3 al. 1 de la directive).

accès à Internet, les prestataires des différents services d'information *on line*, etc.

45. L'article 4 § 1 stipule : "Le prestataire d'un service de télécommunications accessible au public doit prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement, avec le fournisseur du réseau public de télécommunications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant".

Nonobstant le libellé du début de ce paragraphe, les obligations y stipulées ne représentent pas une pure application de la directive générale et de son article 17. Les rédacteurs de la directive "Télécom" ont eu égard aux facteurs de risque plus nombreux liés, d'une part, à la communication par réseau d'un service largement accessible et, d'autre part, à la nature particulière des données, puisqu'il s'agit de données générées par l'utilisation du réseau, données révélant donc les choix des utilisateurs, leurs goûts et offrant en outre l'accès à des données permettant aisément de les contacter.

Le libellé de l'article 4 traduit bien cette préoccupation. Ainsi, la première phase s'achève par l'obligation éventuelle de définir des mesures de sécurité conjointement avec le fournisseur du réseau public de télécommunications.

En ce qui concerne les mesures techniques de sécurité appropriées la seconde phrase du premier paragraphe se réfère non à l'état de l'art en général, comme le fait l'article 17 de la directive générale, mais bien aux possibilités techniques les plus récentes qui doivent garantir un degré de sécurité adapté au risque existant.

A cet égard, on notera le développement de certaines initiatives : l'offre par des serveurs dits d'anonymisation de services permettant aux utilisateurs de services d'Internet de ne pas devoir s'identifier auprès de serveurs ou l'idée de "privacy marker" par lequel le consommateur pourrait indiquer qu'il ne désire pas recevoir de courrier E-mail non sollicité ou voir son adresse communiquée à des tiers[82].

Le second paragraphe ajoute qu'en cas d'existence d'un "risque particulier" de violation de la sécurité du réseau, "le prestataire d'un service de télécommunications accessible au public doit informer les abonnés de ce

---

82 Office of the Data Protection Registrar (U. K.), " Privacy enabling Technologies, Suppression Markers " in *Internet Addresses*, Discussion Paper, March 97.

risque ainsi que de tout moyen éventuel d'y remédier, y compris le coût que cela implique". Le libellé de ce second paragraphe apparaît particulièrement heureux lorsqu'on envisage les risques encourus par l'utilisation d'Internet. On sait notamment qu'un tel réseau de réseaux, de par son caractère ouvert, n'offre que peu de garanties de confidentialité des messages. On conçoit dès lors les fortes recommandations du groupe dit de Berlin[83], à la fois de ne pas utiliser le réseau pour la communication de données sensibles[84] et d'encourager l'anonymat et le cryptage sur le réseau[85]. Au-delà, les traitements dits invisibles que permet Internet appellent des dénominations et des mises en garde particulières. Ces traitements sont de divers ordres; il s'agit du profilage de l'utilisation permis par l'enregistrement de sa navigation sur Internet. Il s'agit ensuite de la possibilité d'inspecter les données stockées sur l'ordinateur contenant le navigateur. Enfin, conséquence des deux premiers risques, le profilage du comportement des navigateurs associés au contrôle des informations se trouvant sur le poste du client permet de mettre sur pied des techniques de sites simulés (*web spoofing*), c'est-à-dire des sites répondant aux besoins détectés a priori par le profilage du navigateur.

47. Ainsi, "les cookies sont des informations que le serveur stocke sur le disque de l'utilisateur sans le prévenir. Le serveur peut interroger le fichier de cookies qui se trouve sur le disque dur de l'utilisateur. Cette fonctionnalité s'apparente en quelque sorte à la mémoire que possèdent les Minitels. Mais le serveur peut également repérer l'historique des pages Web consultées. Cette fonctionnalité est utilisée par les sociétés de

---

83 Il s'agit de l'International Working Group on Data Protection in Telecommunications, groupe rassemblant des membres de Commissions de protection des données et des experts. Ce groupe a émis lors de sa 20e session le 19 nov. 1996, le "Data Protection and Privacy on the Internet - Report and Guidance" dit Budapest-Berlin. Memorandum. Ce rapport est disponible à l'adresse suivante : http : //www. datenschtuz-berlin. de.

84 Cf. le rapport cité note précédente, Guidance n° 2 : "Patients" data and other sensitive personal data should only be communicated via the Internet or be stored on computer linked to the Net if they are encrypted". A noter la condamnation par l'autorité norvégienne de protection des données d'un hôpital qui communiquait sans cryptage avec des centres de recherches scientifiques des résultats d'analyse. Cette condamnation a été remise en cause par un tribunal et fait actuellement l'objet d'un pourvoi devant une juridiction d'appel.

85 "The use of secure encryption methods must become and remain a legitimate option for any user of the Internet". "Anonymity is an essential additional requirement for privacy protection on the Internet".

marketing direct et le "one to marketing, afin de cibler les utilisateurs"[86]. On connaît également les scripts et "applets" JAVA, qui constituent des programmes ou instructions qui sont à votre insu appelés et intégrés dans votre navigateur dans la mesure où des trous de sécurité existent. Ces programmes ou instructions commandées à distance peuvent alors exécuter des recherches ou transcrire certaines informations quant à votre utilisation du navigateur[87].

De tels traitements sont condamnés en vertu du principe de la collecte et du traitement loyal des données prescrit par l'article 6 de la directive. Ils doivent faire l'objet d'informations et de sévères mises en garde par les différents acteurs d'Internet et des autorités de protection des données. La recherche de solutions techniques (ainsi, la version 3. 0. de Netscape et la dernière version de Microsoft Explorer) qui permettent de signaler "en temps réel" le passage des cookies et surtout l'appui y compris des autorités publiques à la diffusion maximale de ces solutions[88] se déduit directement du prescrit de l'article 4 § 2 du projet de directive.

Ces réflexions finales à propos d'Internet[89] introduisent notre conclusion à propos d'une nouvelle dimension de la sécurité.

---

86 Cf. la définition ainsi donnée par le CERT, sur son site F. T. P. (cf. en particulier le point 7. 4.). Cf. également http : // www. netscape. com/newsref/std/cookie-spec. html.

87 Pour un exemple du fonctionnement des Javascripts, cf. http : //www. popco. com/grabtst. html.

88 Une telle solution rejoindrait celle développée par le Gouvernement américain de créer un "Research Technology fund" pour la mise au point et la diffusion des P. I. C. S. (Platform for Internet Content Selection), logiciels permettant de sélectionner automatiquement les sites en fonction d"une labellisation de ces sites. Ces P. I. C. S. ont été développés comme une alternative à un initiative législative réprimant les contenus illicites et indécents sur Internet. On peut imaginer que le développement et la diffusion des solutions techniques semblables aux P. I. C. S. favorisant la protection des données puissent de même être soutenus en matière de protection des données (à ce propos, P. Resnisk, Privacy applications of PICS, Paper prepared for the Federal Trade Commission Public Workshop on consumer Privacy on the G. I. I. , 4-5 juin 96, article disponible à l'adresse suivante http : //www. research. att. Com / - p.resnick / papers / f. t. c. 96. testimony. html.

89 Sur ces diverses questions et solutions techniques, le lecteur se réfèrera à l'article Y. Poullet, Internet et Vie privée, Colloque de Stresa, 1997, à paraître.

EN GUISE DE CONCLUSION, UNE NOUVELLE DIMENSION DE LA SÉCURITÉ

48. Au mois d'août 1995, les autorités de protection des données des Pays Bas et de l'Ontario publiaient un rapport "Privacy Enhancing Technologies"[90]**.** Il s'agissait de décrire certaines techniques susceptibles, lors de l'utilisation de réseaux, de permettre que l'identité de la personne concernée par une transaction ne soit révélée qu'aux seules personnes pour lesquelles cette identité s'avère nécessaire. De ces techniques, on rapproche d'autres. Leur but est que les utilisateurs des réseaux soient à même de contrôler la communication de leurs données personnelles.

Ainsi, en ce qui concerne le premier type de technique, le rapport s'attache à décrire des services ou des techniques dites de "protection de l'identité" (identity protection) par l'utilisation de signatures digitales, de pseudonymes, de tiers de confiance, etc. Ces techniques introduisent entre la personne utilisateur du réseau et certains destinataires du message dont ils ne désirent pas être connus, un filtre qui dissocie le contenu du message de son auteur. Ainsi, les opérateurs de télécommunications voire les fournisseurs d'accès à Internet pourraient offrir aux clients qui le souhaitent, un service de pseudonymes qui permettrait à ces clients de naviguer sur Internet sous couvert d'un pseudonyme.

Le second type de technique, qui permettrait à chacun, lors de l'utilisation de réseau, de maîtriser la circulation des données le concernant se révèle particulièrement utile dans le cadre d'Internet. Le phénomène des cookies, que nous avons déjà évoqué, a provoqué un large émoi dans la communauté des utilisateurs d'Internet. Les cookies permettent de stocker sur l'ordinateur de l'utilisateur les informations relatives à ses habitudes de navigation. Le serveur qui les y a mis pourra les récupérer et les réutiliser lors de passages ultérieurs sur son site**.**

Les protestations des utilisateurs d'Internet ont conduit en particulier les sociétés fabriquant les logiciels de navigation à mettre au point des techniques qui préviennent l'utilisateur préalablement à l'envoi de cookies et lui permettent de s'y opposer. Le même mouvement a persuadé certaines sociétés offrant des sites sur Internet d'avertir leurs utilisateurs de la possibilité de collecte des données d'utilisation de leurs sites et de s'y opposer**.**

49. Ainsi se dessinent de nouveaux droits lors de l'utilisation des réseaux : le droit à l'anonymat et le droit de la personne concernée de décider elle-même de la collecte par autrui de données la concernant. Il

---

90 *supra* note 2, la référence de ce rapport.

s'agit de prévenir la multiplication des lieux de collecte des données générées par l'utilisation des multiples réseaux et services de télécommunication. La sécurité ne s'entend pas de la protection de données déjà collectées contre des utilisations illégitimes ou externes mais de la limitation *a priori* de telles collectes. Elle suppose que le *design* du système d'information prenne en compte une telle exigence[91]. Comme le souligne le récent "Report and Guidance", dit "Budapest Memorandum" adopté par l'International Working Group on Data Protection in Telecommunications" les 15 et 16 avril 1996[92], "It is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop principles for information and communication technology and multimedia hard and software which will enable the individual user to control and give him feedback with regard to his personal data. In general user should have the opportunity to access the Internet without having to several their identity where personal data are not needed to provide a certain service".

50. Le droit de la "sécurité" en matière de protection des données prend ainsi une dimension nouvelle : la technologie permet l'anonymat et mieux, la "contractualisation" de la relation entre l'utilisateur et le serveur. Le premier informé des possibilités de collecte et des finalités du serveur doit pouvoir autoriser ou refuser cette collecte. Se voit ainsi renforcée la maîtrise du sujet sur ses données et consacrée dès lors la participation individuelle des citoyens à la circulation de leur image informationnelle. Il est remarquable de constater que c'est au sein du réseau, par un dialogue, que sont ainsi élaborées des garanties adéquates et une protection effective de notre vie privée.

---

91 A ce propos H. Burkert, A few comments on Privacy Enhancing Technologies, in P. Agree-M. Rotenberg (eds), *Technology and Privacy : the new Landscape,* MIT Press, Cambridge (*Mass*), 1997 ; S. RODOTA, Protecting Privacy in a changing world, Colloque, Bruxelles, 17-18 oct. 1996, Colloque organisé par le CRID, à paraître; P. *A. Strassman, W. Marlow*, Risk-Free Access into the GII via anonymous Remailers, Harv. Univ., Kennedy School of GII project, Symposium on the GII : information, Policy and I. Infrastructure, Cambridge, M. A. , Jan. 28-30, 1996.

92 Sur ce rapport et le working group auteur du rapport, cf. les références précitées.