

**La transposition 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
en
Droit britannique**

Juin 2002



Jurisclope 2002

SOMMAIRE

INTRODUCTION	4
PARTIE I : EXISTE-IL DANS LA TRANSPOSITION BRITANNIQUE DE LA DIRECTIVE 95/46/CE DES DISPOSITIONS S'APPLIQUANT DE MANIERE SPECIFIQUE A INTERNET POUR LES REGLES DE PROTECTION DE DONNEES A CARACTERE PERSONNEL ?	6
PARTIE II : COMMENT LES DISPOSITIONS DE L'ARTICLE 4 DE LA DIRECTIVE 95/46/CE, SUR L'APPLICATION DU DROIT NATIONAL ONT-ELLES ETE TRANSPOSEES ?	7
PARTIE III : L'ARTICLE 20 DE LA DIRECTIVE DEMANDE AUX ETATS DE PRECISER LES TRAITEMENTS SUSCEPTIBLES DE PRESENTER DES RISQUES PARTICULIERS AU REGARD DES DROITS ET LIBERTES DES PERSONNES. QUELS SONT LES TRAITEMENTS QUI EN DROIT NATIONAL SONT SOUMIS A UN CONTROLE PREALABLE ?	9
PARTIE IV : LES ARTICLES 25 ET 26 DE LA DIRECTIVE DEFINISSENT LES CONDITIONS DE TRANSFERT DE DONNEES PERSONNELLES VERS UN PAYS TIERS. QUELLES SONT LES DISPOSITIONS DE DROIT NATIONAL TRANSPOSANT CES DEUX ARTICLES ?	13
PARTIE V : L'ARTICLE 13 DE LA DIRECTIVE PREVOIT DES DEROGATIONS LIMITANT LA PORTEE DES OBLIGATIONS ET DES DROITS DEFINIS A L'ARTICLE 6. QUELLES SONT CES DEROGATIONS EN DROIT NATIONAL ?	17
ANNEXES	22

DOCUMENTS DE REFERENCE*a) Textes législatifs, décrets, etc.*

- ✓ Data Protection Act 1998

b) Documents explicatifs

- ✓ Legal guidance (Guide juridique)
- ✓ Principles (analyses sur les principes de la Data Protection Act)
- ✓ Code of practice (code de bonne pratique)
- ✓ International transfers of personal data (Conseil relatif au respect des conditions du transfert des données à caractère personnel hors du territoire communautaire)

c) Rapports relatifs aux plaintes des particuliers qui ont fait l'objet du traitement

- ✓ Etude des cas
- ✓ Rapport annuel de 1998/1999 et estimations pour les années 1999/2000 à 2003

INTRODUCTION

Les systèmes anglo-saxon tendent à responsabiliser les citoyens. Ainsi, les procédures de contrôle *a priori* ne sont pas dans la tradition du droit anglais. Les autorités publiques préfèrent mettre en place des informations à la disposition des individus pour les guider plus que pour les contraindre : les citoyens informés appliquent le droit en « bon père de famille ». Par conséquent, les individus sont présumés raisonnables, responsables, respectueux de la loi et de bonne foi ; ils bénéficient d'une large liberté d'action.

Il est bon de savoir aussi que, de façon générale, le citoyen britannique n'est pas habitué à une rupture brutale. Il apprécie plutôt une évolution lente du droit. Par conséquent, les changements législatifs imprévus et imprévisibles sont quelque chose de nouveau dans le système juridique anglais. Les directives européennes, qui imposent une obligation de résultat aux Etats membres à travers les lois de transposition, ne sont pas très bien vues. Ainsi, il faudra un temps de transition pour appliquer les règles contraignantes de la Directive 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.

Cependant, la directive européenne du 24 octobre 1995 (95/46/CE) sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données est transposée en Grande-Bretagne. Il s'agit de *Data Protection Act* du 16 juin 1998, qui est entré en vigueur le 1^{er} mars 2000. Il faut rappeler que la Grande Bretagne disposait depuis 1984 d'une loi relative à la protection des données à caractère personnel, qui est abrogée par la nouvelle législation. Par ailleurs, il y avait d'autres lois spéciales qui prévoyaient des règles portant sur la même question. Citons à ce titre « *The financial Services Act 1986* » dont l'article 190 est abrogé par la nouvelle loi, « *The access to personal files Act 1987* » qui est totalement abrogée par la nouvelle loi, « *The access to health records Act 1990* » dont les articles 1(1), 3(1)(a) à (e) et 6(a), 4(1) et (2), 5(1)(a)(i), 10(2), 10(3) sont abrogés par la nouvelle loi, etc.

Les réponses aux questions suivantes sont données sur la base du *Data Protection Act* 1998 et de documents publiés par le Commissaire à l'Information, Elizabeth France.

PARTIE I : EXISTE-IL DANS LA TRANSPOSITION BRITANNIQUE DE LA DIRECTIVE 95/46/CE DES DISPOSITIONS S'APPLIQUANT DE MANIERE SPECIFIQUE A INTERNET POUR LES REGLES DE PROTECTION DE DONNEES A CARACTERE PERSONNEL ?

La transposition anglaise ne comporte pas de disposition spécifique s'appliquant à Internet. Toutefois, il ne fait pas de doute que ce média tombe tout naturellement dans le champ d'application de *Data Protection Act*. Ainsi, il suffit de lire la définition du terme « *data* » (données à caractère personnel) à l'article 1(1)(a) et (b) de la loi britannique :

- sont des données à caractère personnel toute information concernant une personne physique et qui fait l'objet de traitement à l'aide de procédés automatisés.
- de même, à l'article 1(3), il est prévu qu'il importe peu que les données soient traitées immédiatement ou qu'elles doivent intégrer le fichier de données seulement après leur transfert dans un pays hors de la Communauté.

Ces notions de transfert et de traitement automatisé caractérisent les réseaux informatiques en général et Internet en particulier.

PARTIE II : COMMENT LES DISPOSITIONS DE L'ARTICLE 4 DE LA DIRECTIVE 95/46/CE, SUR L'APPLICATION DU DROIT NATIONAL ONT-ELLES ETE TRANSPOSEES ?

A. Les critères transposés

Les dispositions de l'article 4 de la directive sont transposées à l'article 5 de la loi britannique. Ainsi, celle-ci s'applique au responsable du traitement uniquement si celui-ci :

- (a) est installé au Royaume-Uni et si le traitement des données est effectué dans le cadre des activités de son établissement ou ;
- (b) sans être installé au Royaume-Uni ni dans un des Etats membres de la Communauté, utilise des équipements techniques implantés au Royaume-Uni, à des fins de traitement des données, sauf si ces équipements ne sont utilisés qu'à des fins de transit sur le territoire britannique. Selon l'alinéa (2) de l'article 5, dans le cas visé au paragraphe 1 point (b), le responsable du traitement doit désigner un représentant établi sur le territoire britannique.

Par ailleurs, l'alinéa 3 du même article énumère certains cas où le responsable du traitement est réputé établi au Royaume-Uni. Ainsi, sont considérés comme établis sur le territoire britannique :

- (a) un individu qui réside au Royaume-Uni ;
- (b) une entité créée selon la loi du Royaume-Uni ou selon la loi de l'une des composantes du Royaume-Uni ;
- (c) une société commerciale ou autre type de groupement formé selon la loi de l'une des composantes du Royaume-Uni (Ecosse, Pays de Galles...) et
- (d) une personne qui ne serait pas désignée par les dispositions des points (a), (b) et (c) mais :

(i) qui dispose au Royaume-Uni d'un bureau, d'une antenne (filiale, succursale...) ou d'un agence à travers lesquels elle réalise une activité ou ;

(ii) qui opère de façon régulière au Royaume-Uni.

Dans cette dernière hypothèse, la référence aux activités d'un établissement situé dans l'un des Etats membres de la Communauté doit être réelle.

B. Commentaires

Trois remarques :

- 1 – En ce qui concerne l'objet du droit applicable, la loi britannique se veut directe. En effet, l'article 5 prévoit que la *Data Protection Act* 1998 s'applique au responsable du traitement alors que l'article 4 de la directive prévoit que les dispositions nationales s'appliquent principalement aux traitements des données.

- 2 - En ce qui concerne les cas où la loi s'applique, le texte britannique semble vouloir donner une liste strictement limitative. On peut noter cette attitude dans les termes suivants « [...] *this Act applies to a data controller in respect of any data only if...* ». Le terme « *only if* » (uniquement si) souligne le caractère strict de la liste énumérée.

- 3 - Ces cas limités auxquels la loi britannique s'applique signifient *a contrario*, que beaucoup de cas sont exclus de son champs d'application. Mais, l'article 54(3)(b) de la même loi prévoit que le Secrétaire d'Etat britannique doit coopérer avec les autorités des autres membres de la Communauté pour appliquer la loi britannique dans certains cas qui n'entrent pas dans son champs d'application.

PARTIE III : L'ARTICLE 20 DE LA DIRECTIVE DEMANDE AUX ETATS DE PRECISER LES TRAITEMENTS SUSCEPTIBLES DE PRESENTER DES RISQUES PARTICULIERS AU REGARD DES DROITS ET LIBERTES DES PERSONNES. QUELS SONT LES TRAITEMENTS QUI EN DROIT NATIONAL SONT SOUMIS A UN CONTROLE PREALABLE ?

A. Contrôle préalable

La loi britannique, dans son article 22, prévoit une disposition à cet effet. Ainsi, l'alinéa 1 de cet article précise que les traitements visés par cet article sont ceux qui :

- (a) causent un préjudice ou une angoisse substantielle (*substantial distress*¹) à la personne qui fait l'objet du traitement, ou ;
- (b) portent atteinte de façon significative aux droits et aux libertés de la personne subissant ce traitement.

Par conséquent, certains cas de traitement des données à caractère personnel doivent être contrôlés par l'autorité publique compétente : le Commissaire à l'information. Celui-ci est donc chargé d'étudier les demandes d'autorisation du traitement dans certains cas (« *assessable processing* »).

Les conditions d'examen de cette catégorie de traitements sont à déterminer dans un arrêté du Secrétaire d'Etat. Jusqu'à ce jour, ce document n'existe toujours pas. Par conséquent, il appartient au Commissaire d'apprécier au cas par cas les fichiers qui, d'une part, causent un préjudice ou une angoisse substantielle à une personne, ou qui, d'autre part, portent atteinte de façon significative aux droits et aux libertés d'une personne.

¹ La notion de "substantial distress" doit être comprise au sens large. En effet, le législateur aurait pu utiliser la notion de "non-economical damage" (préjudice moral) souvent mise en avant par la jurisprudence, mais en ne le faisant pas, il a visiblement souhaité élargir le spectre d'analyse des fichiers nominatifs soumis à un contrôle préalable.

La question de savoir si la décision du Commissaire est définitive ou peut faire l'objet d'un appel n'est pas résolue par la loi.

B. Procédure de demande d'autorisation

Le responsable du traitement doit (dans les cas où le traitement particulier cause un préjudice ou une angoisse substantielle ou porte atteinte aux droits et aux libertés d'une personne) faire une demande d'autorisation avant la mise en œuvre du traitement. Cette demande est adressée au Commissaire à l'information.

Le « Commissaire » dispose d'un délai de 28 jours à compter de la réception de la demande pour se prononcer sur la qualification à donner au traitement. Cette période d'examen peut être prolongée de 14 jours pour des raisons exceptionnelles non précisées dans la loi. En cas de non-réponse dans les délais (la prolongation doit être notifiée au demandeur pour lui être opposable), il est considéré que l'autorisation est automatiquement accordée. En conséquence, le responsable du traitement peut effectuer le traitement pour lequel il avait demandé l'aval du Commissaire.

C. Les sanctions en cas de non-respect de la procédure de demande d'autorisation préalable

Le responsable du traitement doit respecter la procédure décrite plus haut. Dès lors, le fait de ne pas demander l'autorisation préalable au Commissaire dans les cas où le traitement cause un préjudice ou une angoisse substantielle ou constitue une violation des droits et des libertés d'une personne, ou le fait de ne pas respecter le délai de 28 jours et éventuellement les 14 jours de prolongation fixé pour effectuer le contrôle préalable constitue une infraction pénale (article 21 de la loi).

Le cas échéant, la responsabilité stricte (« *strict liability* ») du responsable du traitement des données à caractère personnel est engagée, sans qu'il soit nécessaire de prouver l'existence d'une intention criminelle. Autrement dit, il est

responsable même si il n'avait pas l'intention de causer l'angoisse, le préjudice et la violation des droits et des libertés des personnes concernées par son traitement. Il ne peut pas non plus échapper à sa responsabilité en démontrant qu'il ignorait les conséquences de ses actes.

Les sanctions encourues varient toutefois selon que le responsable est poursuivi selon une procédure simplifiée (« *summary conviction* ») devant les juridictions de *Magistrates Court* ou selon une procédure non-simplifiée (*indictable offences*) devant les juridictions de *Crown Court*. En effet, c'est la police chargée de mener l'enquête qui détermine la procédure adaptée au cas par cas. Ainsi, si la police choisit la procédure simplifiée, le responsable du traitement sera passible d'une amende de £ 5000. En revanche, si le cas est présenté devant les juges de *Crown Court*, le montant de l'amende sera librement déterminé.

Dans tous les cas, si le responsable du traitement est jugé coupable, la Cour peut ordonner la destruction de tous les matériaux liés à l'infraction. Toutefois, des personnes autres que le coupable, qui se présentent comme les véritables propriétaires de ces matériaux peuvent demander à la Cour la non destruction de ces derniers.

Il faut remarquer également que selon l'article 61, au cas où le responsable du traitement est une société commerciale, le dirigeant (directeur, gérant, secrétaire général ou une personne qui détient des fonctions de décision) est responsable pénalement et solidairement avec la société si l'infraction est commise avec son consentement ou avec sa connivence ; voire si l'infraction est imputable à sa négligence.

De même, si la société est dirigée par l'un de ses membres, celui-ci peut être jugé coupable pour ses actions ou omissions constituant une infraction.

Toutefois, les institutions gouvernementales ne sont pas coupables au même titre que les sociétés commerciales. Ce sont les fonctionnaires qui répondent à titre individuel, selon l'article 55, d'entrave ou de manque de coopération à une procédure judiciaire.

D. Statistiques

Le Commissaire à l'information a publié quelques statistiques sur les demandes d'autorisation préalables ainsi que sur les plaintes des particuliers. En ce qui concerne les cas qui exigent une autorisation préalable, pour l'année 1999/2000 il y'a eu 5 166 demandes d'autorisation préalable ; pour l'année 2000/2001, ce nombre est porté à 8 875. Pour 2002 et 2003, au moins 9000 demandes seront faites selon l'estimation du Commissaire à l'information. Face à cette progression des demandes d'autorisation préalable, celui-ci semble quelque peu débordé. En effet, en 1999/2000, seuls 2 227 dossiers sur 5 166 (43%) ont pas pu être examinés. En 2000/2001, 4 408 dossiers ont été contrôlés sur un total de 8 875 (49%).

Le nombre des plaintes des particuliers est assez important. Ainsi, depuis 1999, on dénombre une moyenne annuelle de 55 000 plaintes enregistrées par téléphone.

**PARTIE IV : LES ARTICLES 25 ET 26 DE LA DIRECTIVE
DEFINISSENT LES CONDITIONS DE TRANSFERT DE DONNEES
PERSONNELLES VERS UN PAYS TIERS. QUELLES SONT LES
DISPOSITIONS DE DROIT NATIONAL TRANSPOSANT CES DEUX
ARTICLES ?**

La loi britannique consacre un des huit principes prévus dans la partie I du « *schedule I* » à cette question de transfert des données vers les pays tiers. En effet, le huitième principe prévoit que les données à caractère personnel ne devront être transférées à un pays non-communautaire que si le pays en question assure un niveau de protection adéquat aux droits et aux libertés des personnes faisant l'objet du traitement.

A. Niveau de protection

La loi britannique donne l'interprétation de ce principe à la partie II du « *schedule I* ». En effet, le niveau de protection adéquat est à déterminer en prenant en considération les points suivants :

- a) la nature des données à caractère personnel ;
- b) le pays ou territoire source de l'information contenue dans les données ;
- c) le pays ou territoire destinataire de l'information ;
- d) les buts pour lesquels et la durée pendant laquelle les données sont traitées ;
- e) la loi (du pays ou territoire destinataire de l'information) applicable en la matière ;
- f) les engagements internationaux du pays ou territoire concernés ;
- g) les codes de conduite et d'autres règles (de portée générale ou spécifique) de ce pays ou territoire ; et
- h) toutes mesures de sécurité prises dans ce pays ou territoire.

B. Dérogations

Le huitième principe ne s'applique pas aux cas prévus au « *schedule 4* » de la loi, sauf certaines exceptions qui seront prévues par un arrêté du Secrétaire d'Etat.

Les cas où le huitième principe ne s'applique pas sont les suivants :

- 1) la personne faisant l'objet du traitement a donné son consentement au transfert de données la concernant ;
- 2) le transfert est nécessaire (a) à l'exécution d'un contrat entre le responsable du traitement et la personne objet du traitement ou (b) à la préparation de la conclusion du contrat et est demandé par la personne objet du traitement elle-même ;
- 3) (a) le transfert est nécessaire à la conclusion d'un contrat entre le responsable du traitement et une personne autre que la personne objet du traitement, (i) si la conclusion du contrat est demandée par la personne objet du traitement ou (ii) si elle faite dans l'intérêt de celle-ci ;
(b) le transfert est nécessaire à l'exécution du contrat ;
- 4) le transfert est justifié par l'intérêt général (le Secrétaire d'Etat doit définir les cas justifiant le transfert dans l'intérêt général) ;
- 5) le transfert est nécessaire (a) pour des raisons judiciaires (b) pour obtenir un conseil juridique ou (c) pour prouver, exercer ou défendre des droits ;
- 6) le transfert est nécessaire à la protection des intérêts vitaux de la personne objet du traitement ;
- 7) le transfert est partie intégrante d'un registre public dont la consultation est ouverte selon des conditions régulières ;
- 8) le transfert est effectué selon des conditions que le Commissaire considère comme adéquat pour protéger les droits et les libertés des personnes objet du traitement, et ;
- 9) le transfert est autorisé par le Commissaire selon une procédure garantissant la protection des droits et des libertés des personnes objet du traitement.

C. Recommandations du Commissaire

A présent, nous voulons attirer l'attention sur un document publié par le Commissaire à l'information² dans le but d'encadrer les activités de transfert des données à caractère personnel. En fait, ce document peut être considéré comme un guide permettant aux responsables du traitement d'entreprendre leurs activités sans violer la loi.

En effet, dans le cadre de transfert de données à caractère personnel, le responsable du traitement doit se poser les questions suivantes :

- Y a-t-il vraiment transfert de données à caractère personnel ?
- Est-ce que la destination se trouve en dehors des pays de l'Union européenne ?
- Est-ce que le pays destinataire est sur une liste de pays qui accordent une protection adéquate aux droits et aux libertés des personnes ?
- Est-ce que l'une ou l'autre exception au principe s'applique ?
- Comment mettre en place un contrat de transfert garantissant la protection des données à caractère personnel ?

Dans tous les cas, la notice explicative considère que l'Australie, Guernesey, Hong Kong, Israël, le Japon, Jersey, la Nouvelle-Zélande, la Pologne, la Slovaquie, la Slovénie et Taiwan disposent d'une protection suffisante des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Aussi, ils peuvent faire partie de la liste des Etats non-communautaires vers lesquels le transfert des données à caractère personnel peut s'effectuer.

² International Transfert of personal data : cf annexe

De plus, pour aider le responsable de traitement dans la rédaction de son contrat de transfert, il est intéressant de noter l'existence de différentes initiatives privées ou publiques :

- un certain nombre d'organisations *professionnelles* (*Chamber of Commerce*, Confédération britannique de l'industrie) ont demandé à la Commission Européenne de valider des modèles de contrat ;
- Au niveau du Royaume-Uni, le Commissaire à l'information veut proposer des modèles de contrat de transfert.
- Dans l'immédiat, le responsable de traitement peut soumettre un contrat au Commissaire, pour approbation.

PARTIE V : L'ARTICLE 13 DE LA DIRECTIVE PREVOIT DES DEROGATIONS LIMITANT LA PORTEE DES OBLIGATIONS ET DES DROITS DEFINIS A L'ARTICLE 6. QUELLES SONT CES DEROGATIONS EN DROIT NATIONAL ?

A. Sécurité nationale

Les articles 27 à 39 de la loi relative à la protection des données à caractère personnel prévoient certaines dérogations.

En effet, l'alinéa 1 de l'article 28 précise que la sauvegarde de la sécurité nationale permet de déroger aux principes présentés à l'article 6 de la directive.

Toutefois, il y a une procédure assez complexe à respecter à cet égard.

Ainsi, le responsable du traitement doit présenter une attestation du Ministre de la Couronne pour bénéficier d'une dérogation justifiée par la sauvegarde de la sécurité nationale. Ladite attestation doit, par le biais d'une description générale, identifier les données à caractère personnel qui font l'objet d'une dérogation.

Il faut noter que la personne qui fait l'objet d'une dérogation peut faire annuler l'attestation ministérielle. Le tribunal peut prononcer l'annulation, s'il trouve que le Ministère ne présente pas de raison valable pour émettre le certificat de dérogations.

L'attestation ministérielle en question peut être :

- un document signé par le Ministre de la Couronne ;
- un document signé au nom et pour le compte de ce Ministre. Le Ministre de la Couronne ne peut pas déléguer pour autant à n'importe quelle autorité publique. Seuls un Ministre faisant partie du cabinet des Ministres, *l'Attorney General* ou le Lord Avocat peuvent bénéficier d'une telle délégation ;

- une copie du certificat original signé par l'une des autorités compétentes.

B. Prévention des crimes et fiscalité

L'article 29 prévoit que le traitement des données à caractère personnel est autorisé s'il est fait pour :

- la prévention ou la détection d'un crime ;
- l'arrestation ou la poursuite des criminels ;
- les contrôles fiscaux, douaniers ou de droits similaires.

En général, les autorités publiques semblent libres de traiter des données à caractère personnel si l'exécution de leur mission en dépend. Ainsi, dans tous les cas où le responsable du traitement est une autorité compétente pour surveiller des personnes à risque en matière de fraude fiscale ou de criminalité, les données à caractère personnel les concernant peuvent être traitées afin de faciliter l'évaluation ou la collecte des impôts, des droits de douane ou de droits comparables. Le traitement des données à caractère personnel concernant les personnes suspectes est également toléré s'il permet de prévenir, détecter leur acte criminel, ou les arrêter et les poursuivre.

C. Santé et éducation

Selon l'article 30 de la loi anglaise, le Secrétaire d'Etat peut libérer de la contrainte de la loi en publiant un arrêté lorsque le responsable du traitement est une autorité publique ou une personne travaillant dans un service public, dans la mesure où le-dit responsable a besoin de traiter les données à caractère personnel pour exécuter ses fonctions légales dans le domaine de la santé, de l'éducation ou du travail social.

Ainsi, le Secrétaire d'Etat peut autoriser la collecte des informations concernant la santé physique ou mentale de certaines personnes. Il peut également autoriser le propriétaire d'une école ou un professeur à traiter les

données concernant leurs élèves. Enfin, les autorités publiques, locales ainsi que certains organismes bénévoles et certains organes désignés par l'arrêté du Secrétaire d'Etat peuvent être exemptés de la contrainte de la loi. A cet égard, la notion d'autorité éducative est à interpréter assez largement.

D. Protection du public

Par ailleurs, l'article 31 prévoit des dérogations accordées aux autorités publiques dont l'exécution des fonctions exige le traitement des données à caractère personnel pour les motifs suivants :

(a) dans un but de la protection des membres de la société contre :

- (i) l'escroquerie en raison de malhonnêteté, de pratiques illicites ou d'autres comportements inappropriés, d'incompétence des personnes impliquées dans les activités d'une banque, d'une assurance, d'un établissement d'investissement ou la direction des sociétés commerciales ;
- (ii) de perte financière en raison d'une faillite ;
- (iii) de malhonnêteté, de pratiques illicites ou d'autres comportements inappropriés, d'incompétence des personnes autorisées à entreprendre une profession ou une autre activité ;

(b) pour protéger les associations humanitaires contre un comportement inapproprié ou une mauvaise gestion ;

(c) pour protéger les biens d'une association humanitaire d'une perte ou d'un mauvais usage ;

(d) pour la récupération des biens d'une association humanitaire ;

(e) pour assurer la santé, la sécurité et le bien-être des personnes dans leur lieu de travail, ou

(f) pour protéger les personnes autres que les travailleurs contre des risques sanitaires et de sécurité en rapport avec les actions des personnes au travail.

Certaines autorités publiques désignées par la loi (art 31 al 4(a)) sont dispensées des contraintes légales pour la mise en place de fichiers de données à caractère personnel pour remplir les missions suivantes : la protection des citoyens contre :

- l'excès de pouvoir de l'administration
- le dysfonctionnement des services publics.

Le directeur général qui contrôle les pratiques commerciales³ peut autoriser le traitement des données à caractère personnel afin de protéger les citoyens contre des pratiques commerciales illicites, pour réguler les ententes commerciales qui compromettent la concurrence ou qui constituent un abus de position dominante.

E. Autres dérogations

Par ailleurs, selon l'article 33, le traitement des données à caractère personnel pour la recherche, l'histoire et les statistiques est autorisé. De même, la mise à la disposition des informations au grand public intervenue en application d'un loi, bénéficie d'une dérogation selon l'article 34.

L'usage domestique (personnel, familial) des données à caractère personnel bénéficie de la même dérogation prévue à l'article 36.

Les publications (journalistiques, littéraires et artistiques) bénéficient d'une dérogation spécifique d'après l'article 32 de la loi anglaise. Toutefois, le responsable du traitement (journaliste, auteur ou artiste) doit être animé par l'idée que la publication (entendue largement et comprend toute mise à la disposition du grand public) répond à un souci de liberté d'expression et est réalisée dans l'intérêt général. Le responsable doit respecter le code de conduite de la profession.

Enfin, l'article 35 rend possible la divulgation des données à caractère personnel à des fins judiciaires, dans la mesure où elles est nécessaire pour établir les droits des parties et pour permettre un meilleur conseil juridique (*legal advice*).

Il faut noter aussi que les articles 38 et 39 de la loi anglaise laissent la possibilité au Secrétaire d'Etat de mettre en place de nouvelles dérogations.

³ Cette institution peut être comparée au Conseil de la concurrence.