

Mélanges offerts au Doyen

Abdelfattah Amor

Tous droits de publications, de traduction et d'adaptation réservés pour
tous pays

© Centre de Publications Universitaires, 2005

B.P. 255, Tunis-Cedex, 1080, Tunis

Téléphone : (216) 874 426 Télécopie : (216) 871 677



CURRICULUM VITAE

Abdelfattah AMOR

Né le 4 mars 1943 à Ksar-Hellal

Marié, père de deux enfants

TITRES ET DIPLÔMES

- Professeur émérite (2004)
- Professeur de l'enseignement supérieur (1979).
- Maître de conférences en Droit Public et Sciences Politiques (1974-1979).
- Maître Assistant (1973-1974).
- Assistant (1970-1973).
- Agrégé en Droit Public et Sciences Politiques (1974).
- Docteur en Droit. Université de Paris II (1973).
- Diplôme d'Études Supérieures en Droit Public. Faculté de droit de Paris (1968).
- Diplôme d'Études Supérieures en Sciences Politiques. Faculté de droit de Paris (1968).
- Licence en droit. Faculté de droit de Tunis (1967).
- Diplôme du cycle moyen de l'École Nationale d'Administration (1967) Tunis.
- Professeur invité aux universités de Paris I, Paris II, Paris V, Nantes, Limoges, Dijon, Bordeaux, Varsovie, Belgrade, Alger, Annaba, Rabat, Casablanca, Fès, Tokyo, Kyoto, Louvain-La Neuve, Colombia university, Harvard Law School .

FONCTIONS UNIVERSITAIRES

- Doyen honoraire de la Faculté des Sciences Juridiques, Politiques et Sociales de Tunis depuis 1993.
- Doyen de la Faculté des Sciences Juridiques, Politiques et Sociales de Tunis (1987-1993).
- Vice-Doyen de la Faculté de Droit et des Sciences Politiques et Économiques de Tunis (1980-1984).
- Directeur de l'Unité d'Études et de Recherches en Droit et Sciences Politiques à la Faculté de Droit et des Sciences Politiques et Économiques de Tunis (1978-1979).
- Secrétaire Général (1984-1988) et Président (depuis 1996) de l'Académie Internationale de Droit constitutionnel.

AUTRES RESPONSABILITÉS ET ACTIVITÉS

- Membre (depuis 1998), vice-président (1999-2003) et Président (depuis 2003) du Comité des Droits de l'Homme des Nations Unies.
- Membre (2000- 2002) et Président (depuis 2002) du jury du prix des Droits de l'Homme de l'UNESCO.
- Rapporteur spécial de la Commission des Droits de l'Homme des Nations Unies sur la liberté de religion ou de conviction (1993-2004).
- Organisateur et Président de la Conférence Internationale Consultative sur la liberté de religion ou de conviction, la tolérance et la non-discrimination (Madrid 2001).
- Participant et intervenant en tant que rapporteur spécial de la Commission des Droits de l'Homme des Nations Unies à la conférence mondiale contre le racisme (Durban 2001).
- Participant et intervenant aux conférences régionales préparatoires à la conférence de Durban de 2001.
- Membre suppléant à la sous-commission de la protection et de la promotion des Droits de l'Homme des Nations Unies (1992-1995).
- Membre du Conseil constitutionnel (1987-1992).
- Membre du bureau de la conférence internationale des doyens francophones (1987-1999).
- Membre du Comité du réseau "Droits Fondamentaux" de l'Aupelf-UREF (1993 - 2003).
- Membre du Comité Exécutif (1987-1991), Vice-Président (1991-1993) et co-Président de l'Association Internationale de Droit constitutionnel (1993-1995).
- Président de l'Association Tunisienne de Droit constitutionnel (1981-2005).
- Expert auprès de la Ligue des États Arabes (1979-1983).
- Président du Jury tunisien d'agrégation en droit public et sciences politiques (1986 et 1999).
- Membre de plusieurs jurys de recrutement pour le grade d'assistant, de maître-assistant, de maître de conférences et de professeur en droit public et sciences politiques.
- Membre du jury algérien d'agrégation en droit public, d'une part, et sciences politiques, d'autre part (1984).
- Secrétaire Général fondateur de l'Association Tunisienne des Sciences Politiques et Sociales (1990-1995).
- Participant en tant que rapporteur spécial de la Commission des Droits de l'Homme des Nations Unies à la conférence mondiale sur les droits de l'homme (Vienne 1993).
- Membre du Conseil National des libertés publiques en Tunisie (1977).
- Membre fondateur de l'Union des juristes arabes (1975).

- Fondateur de plusieurs associations notamment en matière d'environnement, et de culture.
- Membre du jury national d'attribution du prix du 7 novembre.
- Membre du jury national d'attribution du prix de l'innovation administrative.
- Rapporteur général de la Commission Nationale de Protection des Institutions éducatives (1991).
- Membre du Comité de rédaction de la Revue Arabe des Droits de l'homme.
- Membre du Comité de rédaction puis du Comité d'honneur de la Revue Tunisienne de Droit.

DISTINCTIONS ET DÉCORATIONS

- Ordre de la République.
- Ordre du mérite de l'éducation.
- Prix national des droits de l'homme (1998).
- Ordre du mérite civil espagnol.
- Distinctions académiques des universités de Varsovie, Belgrade, Kyoto et Nuremberg.
- Award of Merit of the International Religious Liberty Association

PRINCIPAUX TRAVAUX ET RECHERCHES

- *Manuel de droit constitutionnel* (Al-Wajiz), Tunis CERP, 1987 (en langue arabe).
- *Manuel de droit administratif* (collectif) E.N.A. 1975 (en langue française).
- *Recueil de constitutions et documents politiques tunisiens* (avec K. Saïed), Tunis CERP, 1987 (en langue arabe).
- *Études sur la tolérance* (avec Mohamed Talbi et Néji Baccouche), Tunis, Académie Tunisienne "Beit-el-Hikma" 1995.
- "La démocratie en Afrique", avec Henry Roussillon, *in, les nouvelles constitutions africaines*, Presses de l'Institut d'Études Politiques de Toulouse, 1995.
- *Islam et droits de l'homme* (sous la direction de G. Conac et A. Amor), Paris, Economica 1994.
- *Le suffrage universel* (avec Philippe Ardant et Henri Roussillon), Presse de l'Université des sciences sociales de Toulouse, Toulouse 1994.
- *Le régime politique de la Tunisie*, Paris 1973.
- *Problèmes et perspectives de l'unité maghrébine*, Paris 1968.
- *Le droit constitutionnel saisi par le droit international*, sous presses chez l'Académie tunisienne des sciences, des lettres et des arts.
- *Le droit international et les religions*, sous presses chez Schulthess, Fribourg.
- "Le Comité des Droits de l'Homme des Nations Unies", *in Towards Implementing Universal Human Rights*, Festschrift for the Twenty-Fifth Anniversary

of the Human Rights Committee, edited by Nisuke Ando-Martinus Nijhoff Publishers Leiden/Boston 2004 p. 41.

- “L’ONU et la liberté de religion ou de conviction”, in, *Quelle politique religieuse en Europe et en Méditerranée ? Enjeux et perspectives*, Presses Universitaires d’Aix- Marseille, 2004 p. 13.
- “L’autonomie constitutionnelle aujourd’hui”, in, *Mélanges Pavle Nolic*, Belgrade 2004, p. 21.
- “Intolérance religieuse et discrimination raciale, les discriminations aggravées”, in, *Mélanges Belaïd*, Tunis, CPU 2004, p. 1.
- “Racisme et discrimination raciale”, in, *Premier congrès mondial des droits de l’homme*, UNESCO, Nantes 2004, Sous presse.
- “Le Comité des Droits de l’Homme et le droit constitutionnel”, in, *Recueil des cours de l’Académie Internationale de Droit constitutionnel*, Tunis, Académie Internationale de Droit constitutionnel, 2003, volume 11, p. 1.
- “Le droit de la liberté de religion ou de conviction à l’épreuve des faits”, in, *Mélanges Pierre Pactet*, Paris, Dalloz 2003, p. 19.
- “La condition de la femme au regard de la religion et des traditions”, in, *Mélanges Ben Halima*, Tunis CPU (à paraître).
- *Prévention de l’intolérance religieuse in la libertad religiosa en la education Escolar*, Madrid, Ministerio de Justicia, 2002, p. 19.
- “constitution et élections”, in, *Recueil des cours de l’Académie Internationale de Droit constitutionnel*, volume 10, Tunis, CERES 2002, p1.
- “La religion saisie par le droit : une perspective “droits de l’homme””, in, *Mélanges Mohamed Charfi*, Tunis, CPU 2001, p. 245.
- “Le Comité des droits de l’Homme des Nations Unies : aux confins d’une juridiction internationale des droits de l’homme”, in, *Mélanges Driss Slaoui*, Fondation Al-Saoud, Casablanca, 2000 p. 33.
- “constitution et Droit International”, in, *Recueil de cours de l’Académie Internationale de Droit constitutionnel*, volume 8, Tunis, CPU 2000, p. 5.
- “La constitution tunisienne quarante ans après” (en langue arabe), in, *Le quarantième anniversaire de la constitution tunisienne*, Tunis, CERES 2000, p. 7.
- *L’Assemblée Nationale Constituante 1956-1959*, Tunis, Institut du Mouvement National, 1998.
- “La notion de loi à travers la révision constitutionnelle du 27 octobre 1997”, Sousse, 1998, *Numéro spécial de la Revue des sciences juridiques, économiques et de gestion de Sousse*.
- “Rapport de synthèse sur la révision constitutionnelle du 27 octobre 1997”, Sfax, 1998, *Numéro spécial de la Revue de la Faculté de Droit de Sfax*.
- *Introduction à la révision constitutionnelle du 27 octobre 1997*, Tunis décembre 1997.

- “De la procédure de transmission des avis du Conseil constitutionnel à la Chambre des Députés”, *Revue des Sciences Juridiques, Économiques et de Gestion de Sousse*, n° 1, juin 1997.
- “Rapport introductif” aux *premières journées scientifiques du réseau “droits fondamentaux” de l’Aupelf-Uref*, Publications de l’Aupelf-Uref, Montréal 1997, p. 31.
- “Mandat présidentiel et circonstances politiques particulières”, *Contribution aux journées tuniso-maghrébines de droit constitutionnel*, Tunis, mars 1996.
- “La résistance de la souveraineté : rapport de synthèse”, in, *journées tuniso-françaises de droit constitutionnel*, Tunis, C.P.U. 1998.
- “constitution et religion dans les États musulmans”, *Recueil des cours de l’Académie Internationale de Droit constitutionnel*, Dixième session, Presse de l’Université des sciences sociales de Toulouse, 1996.
- “Éducation et culture politique”, *Revue des Échanges de l’AFIDES*, n° 41.
- “La liberté religieuse”, *R.T.D.*, 1994 (en langue arabe).
- “La justice constitutionnelle dans les pays du tiers monde”, in, *Justice constitutionnelle*, Tunis CERP 1995.
- “Le droit de l’homme au développement”, in, *Effectivité des droits fondamentaux dans les pays de la communauté francophone*, Montréal, Édition Aupelf-Uref, 1994, p. 107.
- “La liberté académique dans les universités arabes”, *Al-Mostaqbal Al-Arabi*, Centre d’études sur l’unité arabe, Beyrouth, n° 1994-12 (en langue arabe).
- “Les droits de l’homme et les changements civilisationnels dans le monde d’aujourd’hui”, *Revue arabe des Droits de l’Homme*, Tunis, I.A.D.H., n° 1 (en langue arabe).
- “Culture politique et démocratie”, in, *L’éducation aux droits de l’homme et la démocratie*, publication de l’I.A.D.H., Tunis, 1994 (en langue arabe).
- “L’enseignement des droits de l’homme dans les facultés de droit dans le monde arabe : rapport introductif” in, *publication de l’I.A.D.H.* sur la même question, Tunis 1993 (en langue arabe).
- “Le renouveau du droit constitutionnel”, *R.T.D.*, 1993 (en langue arabe).
- “L’émergence de la démocratie dans les pays du tiers monde”, in, *l’Afrique en transition vers le pluralisme politique*, Paris, Economica 1993, p55.
- “Présentation de la contribution de René Chapus au droit administratif”, in, *René Chapus : Docteur Honoris Causa des facultés tunisiennes de Droit*. Publication de la Faculté des sciences juridiques, politiques et sociales de Tunis, 1992.
- “La reconnaissance du droit de grève dans les services publics en Tunisie”, in, *Mélanges René Chapus*, Paris, Montchrestien 1992.
- “Démocratie et stabilité politique”, in, *Les changements démocratiques à travers le monde d’aujourd’hui*, Tunis R.C.D, 1990.

- “Existe-t-il un droit de l’homme à l’environnement ?”, in, *La protection juridique de l’environnement*, Publication de la Faculté des sciences juridiques, Tunis, 1990, p. 23.
- “Le droit constitutionnel prospectif”, in, *Journées tuniso-françaises de droit constitutionnel*, Tunis, C.E.R.P., 1990.
- “Les États arabes et le constitutionnalisme”, *R.T.D.*, 1990.
- “constitution et pluralisme politique en Tunisie”, in, *Les expériences constitutionnelles maghrébines*, Tunis, C.E.R.P., 1987.
- “Fédéralisme et décentralisation : rapport de synthèse”, in, *Fédéralisme et décentralisation*, Fribourg, Éditions universitaires, 1987.
- “Les groupes parlementaires”, in, *la Chambre des députés*, Tunis, C.E.R.P., 1986 (en langue arabe).
- “L’Assemblée Nationale Constituante : rapport introductif”, in, *l’Assemblée Nationale Constituante*, Tunis, C.E.R.P., 1986 (en langue arabe).
- “Les droits de l’homme de la troisième génération”, *R.T.D.*, 1985.
- “La question de la succession de Bourguiba”, *R.T.D.*, 1985.
- “La notion d’“Umma” dans les constitutions des États arabes”. *Arabica*, Tome XXX, Fascicule3.
- “La nature du régime politique de la Tunisie”, *R.T.D.*, 1983.
- “La question de l’équilibre entre l’autorité et la liberté dans la constitution tunisienne”, *R.T.D.*, 1983 (en langue arabe).
- “La question du contrôle de la constitutionnalité des lois en Tunisie”, *R.T.D.*, 1982.
- “Rapport introductif sur la réforme du pacte de la Ligue des États Arabes”, *Ouvrage sur la réforme du pacte*, publié à Tunis par le C.E.R.P, 1982 (en langue arabe).
- Chronique constitutionnelle et politique de la Tunisie 1982, *R.T.D.*, 1982.
- Chronique constitutionnelle et politique de la Tunisie 1981, *R.T.D.*, 1981.
- Chronique constitutionnelle et politique de la Tunisie 1980, *R.T.D.*, 1980.
- La constitution tunisienne de 1861, *Revue Servir*, ENA n° 15-16 1974-1975.

RAPPORTS ÉTABLIS DANS LE CADRE DU MANDAT DE LA COMMISSION DES DROITS DE L’HOMME DES NATIONS UNIES SUR LA LIBERTÉ DE RELIGION OU DE CONVICTON

Rapports périodiques présentés à la Commission des Droits de l’Homme

- E/CN.4/1994/79
- E/CN.4/1995/91
- E/CN.4/1996/95

- E/CN.4/1997/91
- E/CN.4/1998/6
- E/CN.4/1999/58
- E/CN.4/2000/65
- E/CN.4/2001/63
- E/CN.4/2002/73
- E/CN.4/2003/66
- E/CN.4/2004/63

Rapports intérimaires présentés à l'Assemblée Générale

- A/50/440
- A/51/542
- A/52/477
- A/53/279
- A/54/386
- A/55/280
- A/56/253
- A/57/274
- A/58/296

Rapports de visite présentés à la Commission des Droits de l'Homme et à l'Assemblée Générale

- Chine E/CN.4/1995/91
- Pakistan E/CN.4/1996/95/add 1
- Iran E/CN.4/1996/95/add 2
- Grèce A/51/542/add 1
- Soudan A/51/542/add 2
- Inde E/CN.4/1997/91/add 1
- Australie E/CN.4/1998/6/add 1
- Allemagne E/CN.4/1998/6/add 2
- États-Unis d'Amérique E/CN.4/1999/58/add 1
- Viet Nam E/CN.4/1999/58/add 2
- Vatican E/CN.4/2000/65
- Turquie A/55/280/add 1
- Bangladesh A/55/280/add 2
- Argentine E/CN.4/2002/73/add 1
- Algérie E/CN.4/2003/66/add 1
- Géorgie E/CN.4/2004/63/add 1
- Roumanie E/CN.4/2004/63/ add 2

COMITÉ D'ORGANISATION

Mohamed Salah **BEN AISSA**
Néji **BACCOUCHE**
Rafaâ **BEN ACHOUR**
Ridha **BEN HAMMED**
Chafik **SAIED**
Ferhat **HORCHANI**
Slim **LAGHMANI**
Neila **CHAABENE**
Kaies **SAIED**
Youssef **HASSEN**
Chawki **GADDES**
Salsabil **KLIBI**
Ghazi **GHERAIRI**

La mise en page de ces mélanges a été conçue et réalisée par les soins de
Chawki Gaddes

SOMMAIRE

Préface	
Sadok BELAÏD	1
Constitution et pouvoir local en Tunisie	
Néji BACCOUCHE	7
La constitution marocaine et ses révisions	
Najib BA MOHAMMED	19
Religious liberty. A neglected dimension of education	
Bert BEACH	33
Le fédéralisme dans le monde d'aujourd'hui	
Gérald-A. BEAUDOIN	41
Le juge, aujourd'hui	
Sadok BELAÏD	55
L'administration et son droit : Quelles mutations ?	
Sana BEN ACHOUR	135
L'attitude de l'islam face au terrorisme	
Rafaâ BEN ACHOUR	145
Le recours pour excès de pouvoir dans tous ses états	
Yadh BEN ACHOUR	159
La définition du contrat administratif dans la jurisprudence du tribunal administratif. Doutes et certitudes	
Mohamed Salah BEN AISSA	175
Les compétences législatives et de contrôle des secondes chambres parlementaires	
Mohamed Ridha BEN HAMMED	193
Partenariat et gouvernance territoriale en Tunisie	
Mustapha BEN LETAIEF	237
Le nouveau cadre juridique des élections législatives au Maroc	
Nadia BERNOUSSI	267
A la recherche de l'internationalité des contrats entièrement intégrés dans l'espace virtuel	
Sami BOSTANJI	279
Pour une convention globale portant sur le droit de l'homme à l'accès à l'eau potable	
Soukaina BOURAOUI	291
Crise de la sécurité sociale et insécurité	
Ezzeddine BOUSLAH	297
Réflexions autour de la composition de la chambre des conseillers en Tunisie	
Amira CHAOUCH	307
Équité fiscale : Les droits de l'État et l'État de droit	
Neïla CHAABANE	321

Culture et droit dans le monde musulman : l'exemple tunisien	
Mohamed CHARFI	333
Droit international privé et droits de l'homme	
Lotfi CHEDLY	353
La démocratie de la noria	
Francis DELPÉRÉE	389
La déclaration universelle des droits de l'homme et le juge tunisien. Vue générale à propos de quelques tendances récentes	
Jamel DIMASSI	399
Du traitement des données personnelles par les personnes publiques en tunisie. Une lecture comparée de la loi n° 2004-63	
Chawki GADDES	417
L'application des notions juridiques indéterminées par le juge administratif tunisien : l'exemple de l'intérêt général	
Ghazi GHERAIRI	473
Cherche droit désespérément dans l'action préventive américaine en Irak	
Nacer-Eddine GHOZALI	487
Les nations unies et la liberté de religion ou de conviction	
Patrice GILLIBERT	503
Religious freedom and inter-religious dialogue : need for more inter-religious dialogue ?	
John GRAZ	521
Comprendre les sens du mot "religion" en droit	
T. Jeremy GUNN	529
Les droits fondamentaux et les constitutions maghrébines	
Salwa HAMROUNI	549
Autonomie constitutionnelle et communauté économique africaine	
Youssef HASSEN	567
Valeur humaine et construction d'un ordre public international	
Maurice KAMTO	583
Autonomie constitutionnelle et droit de la famille	
Monia KARI	605
Autonomie constitutionnelle et théorie générale du droit constitutionnel	
Salsabil KLIBI	615
La question de la justiciabilité des droits économiques, sociaux et culturels	
Hatem KOTRANE	635
L'internationalisation des conflits armés	
Noura KRIDIS	661
Droit international et identité	
Slim LAGHMANI	691
Le gouvernement de la fédération de Russie	
Michel LESAGE	703

Autonomie scolaire et intégration sociale	
José Luis Martínez LOPEZ-MUÑIZ	719
Le système de parti ultra-dominant en Tunisie	
Hatem M'RAD	727
L'Algérie et les droits de l'homme (1962-2003)	
Ahmed MAHIOU	759
L'informatique et la protection de la vie privée	
Farouk MECHRI	783
Le droit international privé sous l'angle de la tolérance	
Ali MEZGHANI	805
Approche critique du code du statut personnel	
Kalthoum MEZIOU	817
Les dispositions constitutionnelles à usage unique	
Mohamed MIDOUN	831
Les droits de propriété intellectuelle et la sécurité alimentaire (Le droit des obtentions végétales)	
Mohamed Larbi Fadhel MOUSSA	859
Le renouvellement contemporain de la notion de constitution	
Pierre PACTET	877
Flux et reflux du réformisme institutionnel de la cinquième république	
Stéphane PIERRE-CAPS	887
La religion dans la constitution pour l'Europe	
Gerhard ROBBERS	897
Les sociétés transnationales et les droits de l'homme	
Mounir SNOUSSI	909
The role of non-governmental organizations in supporting the un strategy for education for tolerance	
John B. TAYLOR	925
La liberté de religion et de conviction : Quels chemins pour demain ? Une perspective globale	
Maurice VERFAILLIE	929
Lumières sur la communauté assyro-chaldéenne syriaque de Turquie	
Joseph YACOUB	939
Constitution et partis politiques en Algérie	
Béchir Yelles CHAOUCH	949
Le comité des droits de l'homme et le défi de Guantanamo	
Alfred De ZAYAS	961
Partie en langue arabe	970

DU TRAITEMENT DES DONNÉES PERSONNELLES PAR LES PERSONNES PUBLIQUES EN TUNISIE

Une étude comparée de la loi organique n° 2004-63

Chawki GADDES *

“Le jour où, au sein de l’État, chaque fonctionnaire qui détient une parcelle de la puissance publique pourrait tout savoir de chaque homme, de chaque famille, de chaque entreprise, ne voit-on pas à quels risques l’administré serait exposé ?”.

Bernard Tricot, *Rapport de la commission informatique et libertés*, 1975, tome 1, p. 17.

INTRODUCTION

Depuis le référendum de mai 2002, le nouvel article 9 de la constitution tunisienne dispose que “l’inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garanties, sauf les cas exceptionnels prévus par la loi”¹. C’est là une disposition importante à plus d’un titre. Cet article fait de la Tunisie le seul État arabe et musulman à constitutionnaliser le principe de la protection des données à caractère personnel. Une pratique pourtant de plus en plus courante de par le monde qui a été amorcée depuis la fin des années soixante-dix².

* Assistant à la Faculté des sciences juridiques, politiques et sociales de Tunis, chargé du cours d’informatique juridique. Secrétaire Général de l’Association tunisienne de droit constitutionnel. Secrétaire exécutif de l’Académie internationale de droit constitutionnel.

¹ Dans son discours de présentation de la révision constitutionnelle de 2002, le Président de la République déclarait que celle-ci permettrait d’“élever certaines libertés à un rang constitutionnel pour leur assurer davantage d’inviolabilité et de protection”, et “assurer aux droits de l’homme une protection efficace qui les mette à l’abri de toute atteinte”. Et de continuer que l’“extension de la protection de la vie privée de l’individu et la consécration de l’inviolabilité des communications et de la protection des données personnelles” est un des buts de cette révision.

Il est intéressant à noter que cette disposition prévoit des dérogations qu’elle considère comme exceptionnelles et qu’il revient donc à la loi de déterminer, ce qu’est censé réaliser la loi 2004-63 objet de notre étude.

² La Tunisie devient avec la nouvelle réforme de la constitution le 28^e pays dans le monde à faire accéder la protection des données personnelles au rang le plus élevé, à savoir le rang constitutionnel. Voir notre étude, “La consécration constitutionnelle de la protection des données à caractère personnel”, in, *Mélanges offerts à Sadok Belaid*, CPU, 2004, Tunis, pp. 363-397. Un tableau porté en annexe de cette étude a été mis à jour grâce à la récente base de données constitutionnelles mise sur pied sous la direction du Doyen Abdelfattah Amor au sein d’une équipe de recherche à l’Académie internationale de droit constitutionnel.

Sur le plan africain, la Tunisie est le deuxième État après le Cap-Vert à constitutionnaliser la protection des données à caractère personnel.

La loi tunisienne, qui s'intègre dans le projet de mise en place d'une société de l'information³, tarda à voir le jour⁴. Comme pour se rattraper, le législateur lui consacra pas moins de cent cinq (105) articles, ce qui constitue un véritable code de la protection des données personnelles. Les cinquante premières dispositions mettent en place le régime général de la protection des données personnelles. Ce sont les règles de droit commun⁵ de la protection des données personnelles qui ne sont d'ailleurs pas spécifiques à la Tunisie. Sur ce plan, le législateur s'est amplement inspiré des expériences étrangères.

Dans un deuxième temps, la loi organique prévoit des exceptions à ce régime général. Son chapitre V⁶ section I est consacré au traitement des données personnelles par les personnes publiques. C'est cette partie de la loi qui fixe les règles suivant lesquelles les personnes publiques vont pouvoir traiter les informations personnelles relatives aux citoyens. Ces dispositions se présentent de par leur position dans le texte, mais aussi à travers l'intitulé du chapitre qui les réunit, comme dérogoatoires au régime général tracé plus haut. En effet, les personnes publiques, dans leurs rapports avec les citoyens sont dotées de plus de pouvoirs que les personnes privées. Cette relation entre les deux parties est par définition inégalitaire au détriment généralement du citoyen. C'est pour cette raison que les règles de protection doivent être plus strictes quand il s'agit de personnes publiques.

En découvrant ce titre, le lecteur s'attend à trouver, dans cette partie, les règles que l'administration tunisienne aura à mettre en œuvre pour réconforter le citoyen sur la protection constitutionnelle du principe énoncé par l'article 9 de la constitution

...” :

3

“
Voir le texte intégral des travaux préparatoires de la séance n° 34 du 21 juillet 2004 sur le serveur de la chambre des députés, <http://www.chambre-dep.tn>, référence 20040721, pp. 1281 à 1318.

⁴ La loi organique 2004-63 a été discutée devant la Chambre des députés le mercredi 21 juillet 2004 et promulguée le 27 juillet. Elle parut au journal officiel trois jours plus tard.

⁵ Les articles 1 à 6 annoncent le principe de protection et définissent les termes utilisés. Les articles 7 et 8 portent sur les actes préalables au traitement, à savoir la déclaration ou l'autorisation. Les articles 9 à 26 passent en revue les obligations à la charge du responsable du traitement des données. Les articles 27 à 43 passent en revue les droits des personnes concernées, à savoir le consentement, le droit d'accès, le droit d'opposition. Les articles 44 à 46 sont réservés aux opérations de collecte, de conservation, d'effacement et de destruction de données. Enfin, les articles 47 à 52 régissent les opérations de communication et de transfert des données personnelles.

⁶ Le chapitre cinq est intitulé “De quelques catégories particulières de traitement” et comporte quatre sections : la première consacrée aux personnes publiques, la deuxième à la santé, la troisième à la recherche scientifique et la dernière à la vidéosurveillance.

et qui permettra de préserver son intimité et sa vie privée. C'est l'étude du régime prévu pour le traitement de ces données personnelles qui constituera l'objet de notre étude. Celle-ci se fera à la lumière, principalement, des dispositions similaires en droit comparé⁷.

Mais avant de traiter au fond notre sujet, un préalable se pose à nous. Il est en effet indispensable de s'arrêter sur la détermination du sens que revêtent deux notions clefs. Celles-ci apparaissent aussi bien dans l'intitulé de la section première du chapitre V de la loi que dans celui de notre étude. Ce sont, d'un côté, les données personnelles (**A**) et, de l'autre, les personnes publiques (**B**).

A. La définition des données à caractère personnel

Derrière les différentes dénominations qu'elle a revêtues⁸, la notion de "données à caractère personnel" a été rarement définie par la doctrine. La seule explication plausible à cela est que tous les textes normatifs prennent, sans exception aucune, la peine de le faire dans leurs premières dispositions.

⁷ Les textes utilisés pour l'étude comparative, au nombre de 45, ont été recueillis principalement sur les sites Internet des structures de contrôle nationaux. Il s'agit des textes concernant les organisations et les États suivants : Allemagne, Argentine, Arménie, Australie, Autriche, Belgique, Bosnie Herzégovine, Canada, Chypre, Commonwealth, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Honk Kong (Chine), Irlande, Islande, Italie, Japon, Lettonie, Lituanie, Luxembourg, Malte, Monaco, Norvège, Nouvelle Zélande, OCDE, ONU, Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume Uni, Slovaquie, Slovénie, Suède, Suisse, Union européenne (convention et directive), Taiwan et Thaïlande. Voir en annexe les références des textes utilisés.

⁸ La même notion a une autre dénomination, qui a vu le jour avec la loi française n° 78-17 du 6 janvier 1978 intitulée informatique et liberté, c'est celle d'information nominative. Certains écrits doutent de la concordance entre les deux expressions. Voir à ce propos, "Les principaux textes applicables", in *Lamy informatique et réseaux*, 2001, p. 313 où l'auteur déclare que les informations nominatives "ne recourent peut-être pas exactement la notion d'informations à caractère personnel ..." mais où il se ravise plus loin à la page 319 pour écrire "quant au fait que la convention parle de données à caractère personnel alors que la loi française s'intéresse aux informations nominatives, il ne faut y attacher une importance qu'il n'a pas". La loi informatique et liberté définit ce type d'information comme étant celle qui permet d'identifier la personne à laquelle elle s'applique. Dans son article 4 on peut lire que "sont réputées nominatives au sens de la présente loi, les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale". Il faut dans ce cas prendre au pied de la lettre le rapport Braibant qui dans le chapitre consacré à la transposition de la directive européenne déclare que la notion de données à caractère personnel "... paraît plus pertinente que celle d'information nominative compte tenu du développement des moyens d'identification indirecte" (Rapport Guy Braibant, *Données personnelles et société de l'information : Rapport au premier ministre sur la transposition en droit français de la directive 95/46*, 3 mars 1998, la documentation française, Paris, 1998). Il est à signaler que la loi du 6 août 2004 révisant le texte de 1978 porte sur "la protection des personnes physiques à l'égard des traitements des données à caractère personnel".

Pour parler de la même notion, d'autres législations utilisent la dénomination de renseignements personnels. Voir la loi canadienne sur la protection des renseignements personnels et des documents électroniques datant du 13 avril 2000 et révisée en 2004.

En passant en revue les divers textes internationaux⁹, régionaux¹⁰ ou nationaux¹¹, on découvre que ces données sont définies par rapport à quatre éléments.

⁹ Aussi bien les lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel adoptée le 23 septembre 1980 que la directive européenne 95/46 CE du 24 octobre 1995 disposent dans les mêmes termes que "par données à caractère personnel, on entend toute information relative à une personne identifiée ou identifiable". Par contre les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel tel qu'adoptés le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95, ne prennent pas la peine de donner une définition à cette notion.

¹⁰ L'article deux de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel adoptée à Strasbourg le 28 janvier 1981, STE n° 108, entrée en vigueur le 1^{er} octobre 1985 ainsi que la Directive 95/45CE du Parlement européen et du Conseil de l'Union Européenne adoptée le 24 octobre 1995 et relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnels (P.E. et C.E., *JOCE*, 23 novembre 1995, n° 1, 281, p. 31) définissent de la même façon les données personnelles. La directive considère qu'on "entend par données à caractère personnel : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale".

¹¹ La loi française n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par la loi du 6 août 2004, dispose dans son alinéa deux de l'article deux que "... Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ...". La loi canadienne de protection des renseignements personnels spécifie dans son article 3 que ceux-ci se définissent comme étant "... Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment : (a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille ; (b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé ; (c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre ; (d) son adresse, ses empreintes digitales ou son groupe sanguin ; (e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement ; (f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur ; (g) les idées ou opinions d'autrui sur lui ; (h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions ; (i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet ...". La loi luxembourgeoise relative à la protection des personnes à l'égard du traitement des données à caractère personnel du 2 août 2002 dispose dans son article 2 que "... toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ("personne concernée") ; une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ...".

• Le premier est en rapport avec le fait qu'il s'agit de "toute information". C'est toute donnée quelque soit sa nature, son contenu, son support ou la forme qu'elle prend. On est loin de la conception restrictive qui transparaît dans la formulation de loi française de 1978. En effet, celle-ci dans son utilisation du libellé de donnée nominative faisait référence au nom et donc à l'information première attachée à toute personne. La jurisprudence de la Commission Nationale Informatique et Liberté en France forgera petit à petit une conception de plus en plus élargie de cette notion. Ainsi, aujourd'hui on ne peut exclure de cette notion que les informations anonymes telles que statistiques ou celles rendues anonymes de manière définitive. Tout le reste est considéré comme des informations pouvant se rapporter à une personne. On n'a qu'à lire l'article 3 de la loi canadienne, cité en note 11, pour se rendre compte de l'étendue de cette notion. Elle va jusqu'à inclure dans cette catégorie n'importe quel numéro ou symbole ou toute autre indication "identificatrice".

La forme que peut prendre cette information, importe peu, puisque cette information peut avoir divers aspects. Il peut ainsi s'agir de textes, de sons ou d'images fixes ou animées. Ces éléments porteurs d'informations peuvent être matériels donc ayant une consistance et se présenter sur des supports papiers, comme c'est le cas du texte, des photos ou des images. Mais ces données peuvent être sous forme immatérielle et prendre la forme d'enregistrements magnétiques ou optiques, comme c'est le cas des sons et des images numérisés ou animés ainsi que des enregistrements informatiques.

• Le deuxième élément permettant de définir les données personnelles a trait à la nature de la personne à laquelle elles sont rattachées. La grande majorité des textes, aussi bien nationaux qu'internationaux, ne prévoit que la protection des personnes physiques. Ce qui n'empêche pas que certaines exceptions existent. C'est le cas par exemple du Luxembourg, de la Suisse ou de l'Italie qui incluent dans le champ d'application de leur loi de protection les personnes morales¹². Mais la plupart du temps, ce sont d'autres techniques juridiques qui s'attachent à préserver les données personnelles des personnes morales.

• Le troisième élément de la définition est que ces informations doivent impérativement permettre d'identifier ou tout au moins de rendre identifiable les person-

¹² Voir le texte italien du 26 février 2004 dont l'article 4.b stipule que les données à caractère personnel sont "toute information concernant une personne physique ou morale, un établissement ou une association, identifiés ou identifiables, directement ou indirectement, par référence à tout genre d'information, y compris un numéro d'identification personnel". Voir aussi la loi luxembourgeoise du 2 août 2002 en son article 2.e qui dispose que ces données sont "toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ; une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique". Voir, enfin, l'article 2 de la loi fédérale suisse sur la protection des données du 19 juin 1992 qui stipule que "la présente loi régit le traitement de données concernant des personnes physiques et morales ...".

nes auxquelles elles se rattachent. Le considérant 26 de la directive européenne est très explicite sur la question. Il dispose en effet que “pour déterminer si une personne est identifiable, il convient de considérer l’ensemble des moyens susceptibles d’être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier les personnes”. En effet, tous les systèmes juridiques considèrent qu’une donnée ne peut être considérée comme permettant d’identifier une personne que si les efforts et les moyens utilisés pour cela sont, dans de pareilles circonstances, considérés comme raisonnables. Car tout acharnement à vouloir à tout prix rechercher des informations sur une personne, conduit inévitablement à trouver certaines données même les plus cachées. Ainsi, une donnée ne peut être considérée comme personnelle, si les moyens mis en œuvre pour identifier la personne concernée sont considérés comme déraisonnables. Une appréciation qui est du ressort des autorités de contrôle et en dernier recours de celle des juges.

- Le quatrième point de la définition a trait à la manière avec laquelle se rapprochement peut être opéré entre l’information et la personne. Les textes parlent d’identification directe ou indirecte. Pour donner un exemple, une adresse postale ou un numéro de téléphone et, à plus forte raison, un numéro de carte d’identité ou de sécurité sociale est considéré comme directement lié à une personne, alors qu’une adresse IP d’ordinateur¹³, l’est de manière indirecte. En effet, celle-ci n’est que l’identifiant d’un ordinateur relié à un réseau. Mais si on peut faire le lien entre cette machine et son utilisateur, l’adresse IP devient une donnée indirectement personnelle. Cette caractéristique des données s’apprécie, ainsi, au cas par cas¹⁴ et elle est pour le moins épineuse¹⁵.

Le législateur tunisien dans sa tâche de rédaction des articles 4 et 5 de la loi organique a bien fait référence aux quatre points détaillés *supra*¹⁶. Pour résumer, on di-

¹³ Tout ordinateur relié à un réseau qu’il soit Internet ou intranet y est identifié par un nom unique. Celui-ci est composé d’une suite de quatre nombres séparés par des points (193.95.68.159). Cet identifiant sur le réseau s’appelle l’adresse IP en référence au protocole de communication utilisé sur le net qui est TCP/IP, autrement dit le *Transfer Control Protocol/Internet Protocol*.

¹⁴ Voir les rapports de la CNIL : Données concernant les malades du SIDA, *7^{ème} rapport d’activité de la CNIL*, 1986, la Documentation française, 1987, pp. 225 et ss. ; les fichiers issus des autocommutateurs téléphoniques, *5^{ème} rapport d’activité de la CNIL*, 1983-84, la Documentation française, Paris, 1985, pp. 109 et ss. ; les données relatives aux cartes à mémoire, *6^{ème} rapport d’activité de la CNIL*, 1986, la Documentation française, Paris, 1987, pp. 44 et ss. ...

¹⁵ Fenoll-Trousseau (M.-P.) et Haas (G.), *Internet et protection des données personnelles*, Litec, Paris, 2001, p. 13.

¹⁶ Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, *Journal Officiel de la République Tunisienne*, n° 61, 30 juillet 2004, pp. 1988-1997 : Article 4. “Au sens de la présente loi, on entend par données à caractère personnel toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d’identifier une personne physique ou la rendent identifiable, à l’exception des informations liées à la vie publique ou considérées comme telles par la loi”. Article 5. “Est réputée identifiable, la personne physique susceptible d’être identifiée, directement ou indirectement, à travers plusieurs données ou symboles

ra ainsi, que les données à caractère personnel sont celles qui permettent de remonter à la personne à laquelle elles s'appliquent ainsi que les informations qui y sont jointes.

Pour être plus explicite et démontrer la masse importante des données personnelles, on essaiera de dénombrer quelques informations de ce type. On pourra, en s'inspirant de la directive européenne¹⁷, dire que ce sont aussi bien le nom et le prénom, que les numéros de sécurité sociale, de carte d'identité nationale, du passeport, du permis de conduire, de carte de crédit, ou même de téléphone. Cela peut porter aussi sur l'adresse postale ou électronique. Mais on pourra ajouter dans l'ère du multimédia des données autres que textuelles telles que la photo et la voix. La liste peut être aussi étendue aux méthodes d'identification modernes telles que l'empreinte digitale, l'adresse I.P., la signature numérique, la photo rétinienne¹⁸ et même le code génétique¹⁹. Mais aussi un film issu, par exemple, d'un système de vidéosurveillance et montrant un visage de personne dans le hall d'une gare ou la plaque minéralogique d'une voiture empruntant un tunnel ou un péage d'autoroute. Sans oublier les fichiers des services monétaires enregistrant les transactions

qui concernent notamment son identité, ses caractéristiques physiques, physiologiques, génétiques, psychologiques, sociales, économiques ou culturelles”.

Voir dans le même sens l'article 2 alinéa 2 cité *supra* (note 11) de la loi 78-17 française du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par la loi du 6 août 2004.

¹⁷ On peut ainsi lire dans une étude de Golvers (L.) intitulée “l'informatique et la protection de la vie privée” paru le 11 janvier 2001 sur le site <http://www.droit-technologie.org> : “La nouvelle loi du 11 décembre 1998, transposant la directive européenne 95/46/CE, a fort heureusement clarifié la situation et introduit des définitions claires et cohérentes des concepts utilisés. C'est ainsi que cette loi entend pour son application : Par “données à caractère personnel”, toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ; Ainsi, des identifiants de personnes physiques tels que n° de carte d'identité, n° de carte de crédit, n° de compte bancaire, n° de sécurité sociale, n° de carte Proton, etc., sont à considérer comme des données à caractère personnel. Il en va de même d'informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne ...”.

¹⁸ Donnée biométrique utilisée dans un système d'identification d'une personne à travers la photo de la rétine (membrane tapissant le fond de l'œil) de son œil. La recherche a en effet démontré que chaque être humain, à l'image de son empreinte digitale unique, possède une photo rétinienne qui le distingue du reste de ses semblables. Les systèmes de reconnaissance rétinienne se sont développés ces dernières années suites au climat d'insécurité et d'attentats qui s'est instauré dans nos sociétés modernes. L'utilisation de ce procédé d'authentification, à l'image de tous les procédés de reconnaissance biométriques, pose le problème de la protection des données à caractère personnel.

¹⁹ La reconnaissance génétique se base sur le fait que toutes les cellules d'un individu contiennent le même ADN. C'est ce qui rend l'individu à partir de cette information identifiable. En effet, l'ADN est une macromolécule présente dans les cellules de tous les êtres vivants qui se reproduit à l'identique quand les cellules se divisent.

commerciales réalisées par une carte de paiement bancaire. Ou les cookies²⁰ qui permettent d'identifier un utilisateur d'ordinateur sur le réseau Internet. Il ne faut surtout pas oublier les données de localisation des téléphones portables ... la liste est longue. Le nombre de ces données est sans cesse croissant, il se développe au rythme des avancées technologiques que subissent inconsciemment nos sociétés modernes.

La deuxième notion utilisée par la loi tunisienne et qui pose un sérieux problème de définition est celle de "personne publique".

B. La définition de la notion de personnes publiques

L'article 53 est le premier article de la section et se charge de délimiter les conditions d'application des dispositions dérogatoires. A ce sujet, il pose des conditions organiques et d'autres fonctionnelles, pour le bénéfice de ce régime, par définition, exceptionnel.

- En ce qui concerne les conditions organiques, c'est-à-dire en liaison avec la délimitation des structures qui profitent de l'application de ces dispositions, l'article 53 traite en deux paragraphes successifs de deux catégories de personnes publiques.

Le paragraphe premier dispose, que ce sont les "autorités publiques, les collectivités locales et les établissements publics à caractère administratif". Ensuite, le deuxième paragraphe, ajoute "... les établissements publics de santé ainsi que les établissements publics n'appartenant pas à la catégorie mentionnée au paragraphe précédent ...". Cette distinction s'explique, comme on le verra *infra*, par la différenciation des régimes dérogatoires applicables à chacune de ses catégories de personnes publiques.

Ainsi, et sur un plan organique, les structures citées englobent toutes les personnes publiques. On retrouve les autorités publiques²¹, les collectivités locales, les établissements à caractère administratif et les établissements publics de santé ainsi que les établissements publics non administratifs. Quelques remarques sont à avancer à ce sujet :

²⁰ Les cookies, qui ont pris le nom d'un biscuit anglo-saxon, sont des petits fichiers informatiques générés par les serveurs Internet et contenant des informations personnelles sur l'ordinateur d'une personne qui se connecte sur le web. Ces fichiers sont stockés généralement à l'insu de l'internaute sur le disque dur de son ordinateur et permettent par l'intermédiaire d'un identifiant unique généré par le serveur de l'identifier à l'occasion de prochaines connexions sur le site auteur du cookies. Les cookies peuvent permettre au serveur de calculer par exemple le temps de connexion sur le site, les pages visitées par l'internaute, les applications installées sur l'ordinateur ... Si l'Internaute s'est identifié lors d'une connexion, le cookies garde ces informations pour l'identifier à l'occasion de ces prochaines connexions. L'utilisateur peut en interdire l'inscription sur le disque ou régler le navigateur à les détruire après chaque connexion. Certains sites internet ne permettent l'accès à certains services que si le navigateur de l'internaute est réglé de manière à accepter ces cookies.

²¹ Le législateur dans la version arabe, qui fait d'ailleurs foi, utilise la notion de " ".

La première remarque est le fruit d'une étude comparatiste. En effet, les textes aussi bien internationaux, régionaux que nationaux, distinguent la plupart du temps plutôt les fichiers du secteur public²² de ceux du secteur privé. Ils effectuent par la suite des distinctions au sein des fichiers publics suivant le domaine d'intervention. On ne comprend pas pourquoi le législateur tunisien a pris la peine de dénombrer ces différentes structures, posant un problème de détermination des autorités mettant sur pied ces fichiers, alors qu'il aurait eu intérêt à utiliser la même notion retrouvée dans le droit comparé.

Cette formulation avec la notion d'autorité publique est à notre avis, pour le moins, inappropriée. En effet, les textes aussi bien tunisiens qu'étrangers, quand ils prennent en charge de dénombrer les personnes publiques, commencent par l'État pour continuer avec les autres structures citées dans l'article 53. Ainsi, et pour ne prendre que quelques exemples, on peut citer le statut général de la fonction publique, qui porte la dénomination de statut des personnels de l'État, des collectivités locales et établissements publics à caractère administratif²³ ou alors le décret réglementant les marchés publics²⁴ où le législateur dénombre l'État, les collectivités locales et les établissements publics. Dans une perspective comparatiste, on peut citer d'autres notions utilisées permettant d'éviter tout équivoque. C'est le cas de la directive 2003 du Parlement européen et du Conseil de l'Union européenne concernant la réutilisation des informations du secteur public²⁵ qui parle plutôt

²² Voir à ce propos, les lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel adoptée le 23 septembre 1980. Le point 2 stipule que "les présentes lignes s'appliquent aux données à caractère personnel, dans les secteurs publics et privé...". Disponible sur le site de l'OCDE à l'adresse web suivante : <http://www1.oecd.org/publications/e-book/9302012e.pdf>. Voir aussi la convention européenne n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981 qui dans son article 3.1. stipule que "Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé". La loi fédérale allemande du premier janvier 2002 portant protection des données personnelles, par contre, parle d'organisme public et les définit comme étant : "... les administrations, les instances judiciaires et les autres institutions de droit public de l'État fédéral, des autorités, établissements publics et fondations publiques qui sont directement rattachés à l'État fédéral ainsi que leurs associations, nonobstant leur forme juridique ...".

²³ La loi du 12 décembre 1983 portant statut des personnels de l'État, des collectivités locales et établissements publics à caractère administratif.

²⁴ Cette énumération est à rapprocher de celle contenue dans d'autres textes comme le décret n° 89-442 portant réglementation des marchés publics tel que modifié par le décret n° 97-551 du 31 mars 1997 qui dispose à ce propos que ce sont les contrats passés par "... l'État, les collectivités publiques locales, les établissements à caractère administratif, les établissements publics à caractère non administratif définis par l'article 33-7 de la loi n° 89-9 du 1^{er} février 1989 ... ou les entreprises publiques ...", *JORT*, 4 avril 1997, n° 27, p. 548.

²⁵ Voir la directive 2003/98/CE du Parlement européen et du conseil de l'Union européenne du 17 novembre 2003 concernant la réutilisation des informations du secteur public dont l'article 2 dispose : "Aux fins de la présente directive, on entend par : 1) "organismes du secteur public", l'État, les collectivités territoriales, les organismes de droit public et les associations formées par une ou plusieurs de ces collectivités ou un ou plusieurs de ces organismes de droit public; 2) "organisme de droit pu-

d'organisme du secteur public ou de droit public en prenant la peine d'en définir les contours.

La loi française de 1978 est à ce propos plus explicite. On peut, en effet, y lire dans l'article 27-I-1 qu'il s'agit des "... traitements de données à caractère personnel mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public ...". Ainsi, sans équivoque, le législateur français a passé en revue toutes les personnes qualifiées comme étant du secteur public. Dans ce sens, on peut lire sous la plume de Huet et Maisl que "par secteur public, on entend les différentes personnes morales de droit public [et de les dénombrer en citant] : État, collectivités territoriales, établissements publics et organismes privés gérant un service public ..."²⁶.

Si on revient à la doctrine, la notion d'autorité publique est définie comme étant l'État et les collectivités territoriales²⁷. Dans les textes internationaux, on peut lire dans la convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement que "L'expression "autorité publique" désigne : a) L'administration publique à l'échelon national ou régional"²⁸.

L'alinéa deux du même article 53 continu par la suite pour déclarer que : "Les dispositions de la présente section s'appliquent, en outre, au traitement des données à caractère personnel réalisé par les établissements publics de santé ...". En parcourant cette disposition, on pense dans un premier temps qu'elle concerne uniquement cette catégorie d'établissements publics, qui ne rentrent d'ailleurs pas dans la catégorie citée plus haut des établissements publics à caractère administratif. Mais celle-ci va plus loin puisqu'elle continue en ajoutant "... les établissements publics n'appartenant pas à la catégorie mentionnée au paragraphe précédent ..."²⁹. Donc

blic", tout organisme : a) créé pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial, et b) doté de la personnalité juridique, et c) dont soit l'activité est financée majoritairement par l'État, les collectivités territoriales ou d'autres organismes de droit public, soit la gestion est soumise à un contrôle par ces derniers, soit l'organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les collectivités territoriales ou d'autres organismes de droit public". Journal officiel de l'Union européenne du 31 décembre 2003, L 345/90, disponible à l'adresse http://www.internet-observatory.be/internet_observatory/pdf/legislation/dir_2003-11-17_fr.pdf

²⁶ Huet (J.) et Maisl (M.), *Droit de l'informatique et des télécommunications*, Litec, Paris, 1989, p. 172.

²⁷ Georgel (J.), "Le recours pour excès de pouvoir", *Jurisclasseur administratif*, fascicule 1140, au paragraphe 21 on peut lire que : "... sont autorités publiques, l'État, la région, la commune, le département, la collectivité territoriale d'outre-mer".

²⁸ Voir, convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement du 25 juin 1998 disponible à l'adresse web suivante : <http://www.unece.org/env/pp/documents/cep43f.pdf>

²⁹ "... المؤسسات العمومية للصحة وكذلك المؤسسات العمومية التي لا تنتمي إلى الصنف المذكور بالفقرة المتقدمة..."

cet alinéa regroupe les établissements publics de santé (EPS) ainsi que les établissements publics non administratifs³⁰ dont la liste est arrêtée par décret.

Ce deuxième paragraphe élargit, ainsi, encore plus le cercle des structures bénéficiaires des dérogations prévues par la loi. Ainsi on obtient deux groupes différents de personnes publiques. A chaque groupe la loi appliquera un régime différent.

Mais le bénéfice de ces dérogations est soumis à d'autres conditions, qui sont cette fois-ci fonction non pas de la nature de la structure qui en bénéficie mais plutôt de la nature du domaine dans lequel elles agissent. Ces conditions ont les qualifient de matérielles.

- Le paragraphe premier de l'article 53 fait bénéficier cette dérogation au premier groupe de personnes publiques "dans le cadre de la sécurité publique ou de la défense nationale, ou pour procéder aux poursuites pénales ...". Ce sont là les trois domaines auxquels les expériences comparées³¹ réservent des régimes spécifiques.

Le meilleur exemple qui synthétise ses possibilités apparaît dans l'article 9 de la convention européenne qui est réservée aux exceptions et restrictions pouvant être portées aux règles de protection spécifiées. La dérogation à ces règles est permise lorsqu'elle est "prévue par la loi de la Partie" et quand elle "constitue une mesure nécessaire dans une société démocratique" en vue de "la protection de la sécurité

³⁰ À propos des difficultés de la distinction en Tunisie entre établissement public administratif (EPA) et celle d'établissement public non administratif (EPNA) voir Midoun (M.), "les établissements publics à caractère non administratif : des établissements publics de troisième type ?", in, *Mélanges en l'honneur de Habib Ayadi*, CPU, 2000, pp. 665-717 et Ben Aissa (M.S.), "le champ d'application du décret n° 89-442 du 22 avril 1989 portant réglementation des marchés publics", in, *Mélanges en l'honneur de Habib Ayadi*, CPU, 2000, pp. 215-244.

³¹ Voir l'article 32.V de la loi française du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, telle que modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004 qui dispose que : "V. Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en oeuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté". Voir également l'article 4 de la loi italienne numéro 675 du 31 décembre 1996 qui traite des traitements dans le secteur public et qui dispose que : "1. La présente loi ne s'applique pas à l'égard des traitements de données à caractère personnel effectués : ... e) par d'autres organismes publics aux fins de défense ou de sûreté de l'État ou de prévention, de constatation ou de répression d'infractions, sur la base de dispositions de loi spécifiques prévoyant expressément le traitement. C'est aussi le cas pour l'article 3 de la loi luxembourgeoise du 2 août 2002 qui dispose que "la présente loi s'applique au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, même liées à un intérêt économique ou financier important de l'État, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines". Se référer également à l'article 3 de la loi n° 77/2000 d'Islande (Act on Protection of Individuals with regard to the Processing of Personal Data) qui dispose que : "the provisions of Sections 16, 18 to 21, 24, 26, 31 and 32 shall not apply to the processing of personal data relating to public security, national defence, state security, or the activities of the state's criminal justice system" ...

de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales³².

Ces dérogations se justifient dans ces systèmes démocratiques par les impératifs de bon fonctionnement de certains services de l'État dans des secteurs particuliers. Des domaines qui ont besoin d'un certain degré de secret. Mais il ne faut pas croire que ces dérogations déchargent les personnes publiques de toute obligation, au contraire, les législateurs les ont entourées de gardes fous qui sont de nature à freiner le pouvoir absolu des structures qui en bénéficient. Ces régimes spécifiques seront étudiés plus amplement dans les développements à venir.

Ce qui paraît étonnant dans la loi tunisienne, c'est que l'article 53 ne s'arrête pas à ce niveau, mais va plus loin. En effet, il ajoute "... ou lorsque ledit traitement s'avère nécessaire à l'exécution de leurs missions conformément aux lois en vigueur". L'article de conjonction utilisé est le "ou"³³ qui peut être remplacé par "soit". Dans ce cas la dérogation est étendue à toute l'activité des structures désignées. On ne comprend plus pourquoi le texte détermine des domaines particuliers pour élargir après cela cette dérogation à toute l'activité de ces structures. La seule explication plausible est la suivante : le législateur a voulu citer des domaines généralement constatés dans les législations étrangères mais sans s'y limiter.

Pour être concret, prenons un exemple. La municipalité de l'Ariana, qui est une collectivité locale détient, comme toutes les collectivités locales, un fichier, aujourd'hui informatisé, pour gérer la perception des taxes locatives relatives aux locaux servant à l'habitation dans le périmètre communal. Ce fichier contient, indubitablement et sans aucun doute, des données à caractère personnel de citoyens. Cette personne publique rentre dans la catégorie déterminée dans le premier paragraphe de l'article 53. Mais la gestion de ce fichier ne correspond pas aux conditions fonctionnelles posées par le même article. En effet, la gestion des taxes locatives, n'est ni une affaire de sécurité publique ou de défense nationale et ne rentre pas dans le cadre de la gestion des poursuites pénales. Par contre ce "traitement s'avère nécessaire à l'exécution" de sa mission, il bénéficie de ce fait des dispositions dérogatoire de la section première du chapitre cinq de la loi de 2004. C'est là une extension des dérogations qui ne peut avoir de justifications convaincantes.

Cette interprétation est confirmée par la réponse du ministre de la justice et des droits de l'homme à une question qui lui a été posée par un député³⁴ et qui est re-

³² Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel adoptée à Strasbourg le 28 janvier 1981, STE n° 108, entrée en vigueur le premier octobre 1985.

³³ "... أو كلما كانت تلك المعالجة ضرورية لتنفيذ المهام التي تقوم بها طبقاً للقوانين الجاري بها العمل".
³⁴ السيد محمد المختار الجليلي ما هي الضمانات التي يؤسسها أو يؤسس لها هذا القانون الأساسي بالنسبة إلى المعطيات الشخصية عندما يتعلق الأمر بالسلطات العمومية وعموما بالأشخاص الوارد ذكرهم بالفصل 53 ؟
 السيد وزير العدل وحقوق الإنسان أولاً بالنسبة إلى الأشخاص، السلطات العمومية والجماعات العمومية المحلية، فهي غير مستثناة من كل القانون مثلما قلت بل مستثناة من بعض الأحكام، وهي مستثناة من بعض أحكامه ليس بصفة مطلقة بل هي مستثناة من بعض

prise dans les travaux préparatoires de la loi. Le ministre atteste que les dérogations sont limitées à ces structures, on en convient, mais d'ajouter que c'est une dérogation loin d'être générale !!! Est-ce que la plume du "législateur" a dépassé sa pensée ?

Quant au deuxième groupe de personnes publiques (les établissements publics de santé ainsi que les établissements publics n'appartenant pas à la catégorie des établissements visés dans l'alinéa premier qui sont ceux administratifs), celles-ci ne bénéficient des dispositions dérogatoires que quand elles agissent "... dans le cadre des missions qu'ils assurent en disposant des prérogatives de la puissance publique conformément à la législation en vigueur". Ce genre de dispositions est de nature à poser des problèmes pratiques d'interprétation et de ce fait d'application. En effet, c'est au cas par cas, qu'on devra déterminer si un établissement doit ou non bénéficier des dérogations. S'il s'avère qu'il a agit dans ses relations avec le citoyen comme un simple particulier, il sera soumis au régime général de protection des données personnelles. Si par contre il use des prérogatives publiques qui lui sont octroyées par la législation pour mener à bien sa mission, il bénéficiera de ces dérogations.

Dans ce contexte, il se posera la question de savoir quelle structure est habilitée à déterminer en pratique ces cas ? La réponse nous paraît être que c'est l'Instance Nationale de protection des données personnelles. La loi organique de 2004 lui confère, en effet, la compétence de statuer sur les litiges qui naissent de son application. L'instance développera, au vu des requêtes introduites par les citoyens, une jurisprudence dans laquelle elle éclaircira cette condition fonctionnelle.

Au vu de ce qui précède, la question qui se pose à nous dans le cadre de notre étude est de savoir comment est-ce que les personnes publiques et à quelles conditions elles seront autorisées à traiter des données à caractère personnel des citoyens. La question est d'importance, car les personnes publiques dont une grande part est dénommée "l'administration publique" sont aujourd'hui de très grandes consommatrices de données de ce type nécessaires à son efficacité et devenu aisé grâce au développement des technologies de traitement de l'information. La mise en place en Tunisie, à l'instar de tous les pays du monde, d'un projet d'administration électro-

أحكامه في إطار الأمن العام أو الدفاع الوطني أو القيام بتتبعات جزائية أو كلما كانت تلك المعالجة ضرورية لتنفيذ المهام التي يضبطها القانون حتى نوضح الأمور، أي أن الاستثناء ليس كاملاً والاستثناء ليس مطلقاً لهذه السلطات بل هو محدد بمجالات ضبطها القانون. ما هي الضمانات؟ طبعاً القانون التونسي يوفر عديد الضمانات، وأهم ضمان يوفره القانون التونسي هو دعوى تجاوز السلطة ودعوى الإلغاء التي ترفع أمام القضاء الإداري، وإذا تمت المعالجة أو صدر قرار فيه مخالفة لهذا القانون فهناك ضمان أمام القضاء الإداري، يمكن أن يلجأ إلى القضاء الإداري، ونحن نعلم أن القضاء الإداري إذا حدث أي تجاوز أو أية مخالفة للقانون من قبل الإدارة فإنه يلغي القرارات المؤسسة على هذه المخالفة وشكراً السيد الرئيس.

A ce propos, il est légitime de se demander comment est-ce que le citoyen pourrait tenter un recours pour excès de pouvoir en d'absence d'illégalité dans l'acte administratif incriminé. En effet, l'administration n'ayant aucune obligation à sa charge, elle ne pourra commettre des actes attaquables par le biais de cette voie de recours !!!

nique³⁵ va accentuer ce genre de traitement et de ce fait mettre en danger la vie privée des individus.

En passant en revue les dispositions contenues dans cette section dérogatoire de la loi tunisienne on remarque que celle-ci crée deux régimes spécifiques au bénéfice des deux catégories de personnes publiques déterminées par l'article 53. En effet, toutes les personnes publiques ne sont pas "logées à la même enseigne". Car la loi institue un régime dérogatoire général applicable à toutes les personnes publiques sans aucune distinction. Elle réserve par la suite un régime "hyperdérogatoire" pour la catégorie de personnes publiques déterminée dans l'alinéa premier de l'article 53.

Ainsi à travers les dispositions de la section la loi organique de 2004 vide tout le régime général de protection de ses obligations les plus significatives. Le législateur, quand il s'agit de personnes publiques, ne prévoit aucune garantie de protection des droits des citoyens dans le cadre du traitement de leurs données à caractère personnel. Ainsi de manière générale l'administration se retrouve déchargée des obligations les plus importantes (I), le législateur ira plus loin puisque les membres du premier groupe de personnes publiques profiteront de dérogations supplémentaires touchant les données les plus sensibles (II).

I. UN TRAITEMENT PUBLIC DES DONNÉES PERSONNELLES DISPENSÉ DE TOUTE OBLIGATION

Les personnes publiques comme tout intervenant dans la société doit normalement être soumise aux règles mises en place dans le cadre du régime général de protection des données personnelles. Les exceptions et les restrictions dont elles peuvent bénéficier doivent être limitées aux stricts besoins nécessités par les impératifs de bonne marche des structures publiques. Ces dérogations doivent ainsi être entourées de garanties suffisantes permettant de protéger la vie privée des individus et éviter que l'administration n'acquière des pouvoirs exorbitants qui sont de nature à léser les droits liés à la protection de la vie privée des individus. Les droits internes

³⁵ L'administration électronique est définie aussi bien par l'OCDE comme étant l'utilisation des technologies de l'information et de la communication comme outil pour arriver à une meilleure administration. Voir à cet effet, le rapport de l'OCDE dénommé *l'administration électronique, un impératif*, publications de l'OCDE, 2004, ISBN 92-64-107-85-1, p. 11. Dans la même référence, le rapport à sa page 24 annonce que cette dénomination n'est pas universelle et qu'elle dépend des priorités arrêtées à ce projet. C'est ainsi qu'en Tunisie le projet d'administration électronique a été autrement dénommé puisque sous nos cieux, ce projet a été qualifié de communicante plutôt que d'électronique. Les définitions tournent autour de trois catégories qui dépendent de la volonté politique qui a mis en place ce projet de développement de l'administration électronique. Dans le rapport de l'OCDE, les experts considèrent qu'il y a à ce sujet trois catégories de définitions : la première met en exergue la fourniture de services par l'administration à travers, entre autre, Internet, la deuxième est l'utilisation de manière générale des TIC dans l'activité administrative et enfin la troisième a comme priorité la réforme de l'administration publique par l'utilisation des TIC. Voir rapport *idem*, p. 25.

sont exhortés d'après la résolution 45/95 de l'assemblée générale des Nations Unies à édicter à ce propos des "garanties appropriées"³⁶.

En droit comparé, les législations établissent des règles, aujourd'hui généralisées, qui permettent à l'individu de voir ses données les plus "intimes" protégées, surtout quand il se retrouve devant des personnes publiques³⁷. La loi organique tunisienne a commencé, à travers les dispositions du chapitre deuxième, par mettre en place un régime général de protection des données personnelles. Les règles qui y sont insérées sont principalement les suivantes :

- Demande d'autorisation ou simplement la déclaration du traitement auprès de la structure de contrôle (articles 7 et 8),
- Obligations de respecter certaines règles concernant les données collectées, celles-ci doivent être adéquates, pertinentes, non excessives et dont le traitement doit être loyal et licite (articles 10 et 11),
- Des règles spécifiques pour la collecte et le traitement des données dites sensibles (articles 14 et 15),
- Obligation d'assurer la sécurité et la confidentialité des données collectées (articles 18, 19 et 23),
- Obligation de recueillir le consentement de la personne concernée (articles 27 et 28),
- Droit d'accès aux données collectées (articles 32 et suivants),
- Droit de s'opposer au traitement des données collectées (articles 42 et 43),
- Règles strictes concernant la communication et le transfert des données collectées (47 et suivants),

³⁶ Voir les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel approuvés par la résolution 45/95 de l'assemblée générale des Nations Unies en date du 14 décembre 1990 : "6. Faculté de dérogation. Des dérogations aux principes 1 à 4 [principe de licéité et de loyauté, principe d'exactitude, principe de finalité, principe d'accès] ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées".

³⁷ On peut lire dans l'exposé des motifs un rapport sur la question soumis au Sénat Français ce qui suit : "La France a été l'un des premiers États à introduire dans sa législation des dispositions protégeant les personnes physiques contre les risques induits par l'informatique sur leur vie privée. Tout d'abord, cette menace a été perçue comme susceptible de provenir d'un État-Léviathan. La loi du 6 janvier 1978 a donc distingué les traitements publics réputés plus dangereux et les traitements privés bénéficiant d'une présomption d'innocuité, cette distinction organique étant tempérée par une distinction matérielle entre traitements de données sensibles et traitements courants ne comportant manifestement pas d'atteinte aux libertés". Turk (A.), *Protection des personnes physiques à l'égard des traitements de données à caractère personnel*, Sénat, Rapport 218 (2002-2003), commission des lois, <http://www.senat.fr/rap/102-218/102-2181.pdf>.

- Droit de rectification, de clarification, de mise à jour ou de suppression des données collectées (article 21).

Qu'en est-il de ses obligations en ce qui concerne les personnes publiques ? L'article 54 dans son paragraphe premier dispense les personnes publiques définies dans l'article 53 de certaines obligations qui se retrouvent être les plus importantes pour la protection des données personnelles des citoyens. Par un seul trait de plume le législateur a ainsi fait disparaître toutes les obligations à la charge du titulaire du traitement quand il s'agit d'une personne publique. L'article déclare, en effet, que "le traitement réalisé par les personnes mentionnées à l'article précédent n'est pas soumis aux dispositions prévues par les articles 7, 8, 13, 27, 28, 37, 44 et 49 de la présente loi ...".

Ce que l'on remarque à travers l'étude des dispositions écartées par le législateur, c'est que les personnes publiques, toutes catégories confondues, sont dispensées de toute publicité concernant les traitements qu'elles mettent en place des données personnelles des individus (A). Ces personnes sont également dispensées de toute demande d'autorisation à l'Instance de protection (B). Elles se trouvent aussi dispensées d'obtenir le consentement préalable aux opérations de traitement (C). Il est enfin à noter que les personnes publiques de manière générale profitent d'une autre dispense qui est celle de l'interdiction de traiter des infractions et des peines (D).

A. Des fichiers secrets ou de la dispense de publicité

Le principe est que toute personne qui a l'intention de collecter et de traiter des informations personnelles doit préalablement à cette opération en faire déclaration auprès de la structure de contrôle qui en Tunisie a pris, d'après la loi, le nom d'Instance Nationale de protection des données personnelles³⁸.

Le législateur tunisien a réservé un des premiers articles de la loi à cette obligation. En effet, l'article 7³⁹ en disposant que toute opération de traitement est soumise à une obligation préalable de déclaration fait de cette obligation un principe général. C'est d'ailleurs dans une section dénommée "des procédures préliminaires du traitement des données à caractère personnel" que cette disposition a été placée.

En droit comparé la même obligation est placée au début de chaque texte organisant la protection des données personnelles⁴⁰. Cette déclaration permet à la struc-

³⁸ D'après l'article 6 de la loi tunisienne, "au sens de la présente loi, en entend par ... l'Instance : l'Instance Nationale de Protection des Données à Caractère Personnel ...".

³⁹ L'article 7 de la loi tunisienne dispose que : "Toute opération de traitement des données à caractère personnel est soumise à une déclaration préalable déposée au siège de l'instance nationale de protection des données à caractère personnel contre récépissé ou notifiée par lettre recommandée avec accusé de réception ou par tout autre moyen laissant une trace écrite ...".

⁴⁰ Voir l'article 21 de la directive du Conseil de l'Europe adopté le 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnels, P.E. et C.E., JOCE 23 novembre 1995, n° 1, 281, p. 31. "Publicité des traitements. 1. Les États membres prennent des mesures pour assurer la publicité des traitements. 2. Les États membres prévoient que

ture de contrôle d'être informé de la finalité du traitement ainsi que du contenu du fichier, sa localisation, ses responsables. Autant d'éléments qui sont à même de permettre à cette structure d'exercer un contrôle sur la manière avec laquelle le traitement des données est mis en place et se déroule plus tard.

Le fondement de cette obligation se retrouve aussi dans le souci de permettre aux personnes concernées de connaître l'existence des fichiers et de pouvoir ainsi y accéder et en contrôler, de ce fait, le contenu. "Le créateur du fichier ayant une obligation de transparence, l'information doit se faire au moment de la collecte. Dans le secteur public, il se manifeste par le fait que l'administration doit publier le traitement qui a eu lieu ... C'est le droit le plus important car il conditionne tous les autres"⁴¹. Ceci se comprend bien, car comment pourrait-on contrôler le contenu de quelque chose qui est tenue secrète ? La première obligation est sans conteste celle de rendre public la naissance du fichier.

Le législateur tunisien a opté pour le choix de soustraire les structures publiques à cette obligation puisque l'article 54 stipule que : "Le traitement réalisé par les personnes mentionnées à l'article précédent n'est pas soumis aux dispositions prévues par les articles 7, ...". Ceci équivaut à une dispense de déclaration de la part des administrations publiques. Cette dispense aura pour conséquence qu'aucune publicité ne sera ainsi donnée à ces fichiers. Ces outils de travail que sont les fichiers de données sont aujourd'hui nécessaires dans toute organisation administrative. Des fichiers qui sont appelés à se développer au sein de l'administration et que

l'autorité de contrôle tient un registre des traitements notifiés en vertu de l'article 18. Le registre contient au minimum les informations énumérées à l'article 19 paragraphe 1 points a) à e). Le registre peut être consulté par toute personne ...". Voir aussi loi belge du 8 décembre 1992 qui dispose dans son article 17 § 1^{er} que "préalablement à la mise en oeuvre d'un traitement ... le responsable du traitement ou, le cas échéant, son représentant, en fait la déclaration auprès de la Commission de la protection de la vie privée ...". La même démarche a été suivie par le nouvel article 22 de la loi française (Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004) qui stipule que : "I. A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés ...". L'article 7 de la loi italienne, numéro 675 du 31 décembre 1996 stipule dans le même sens que : "1. Le titulaire ayant l'intention de procéder à un traitement de données à caractère personnel qui rentre dans le champ d'application de la présente loi est tenu à le notifier au *Garante*". Enfin se référer à l'article 4d de la loi fédérale allemande du premier janvier 2002 stipule que "préalablement à la mise en oeuvre de procédures de traitements automatisés, les organismes privés responsables relevant de l'autorité de contrôle compétente et les organismes publics responsables relevant de l'État fédéral ainsi que les entreprises du secteur des postes et télécommunications doivent adresser une notification au Délégué fédéral pour la protection des données, conformément à l'article 4e".

⁴¹ Prebissy-Schnall (C.), *L'Administration électronique et la protection des données personnelles*, 25 janvier 2004, cours publié sur le site e-juriste à l'adresse http://60gp.ovh.net/~ejuriste/article.php3?id_article=134

l'administration électronique, ou communicante comme on se plaît à l'appeler en Tunisie, ne pourra qu'en accroître le nombre.

Au principe général de déclaration que l'on retrouve dans les législations comparées, on instaure au profit des structures publiques certaines dérogations. Celles-ci ne sont pas motivées par la volonté de dispenser l'administration publique de toute obligation, au contraire elles découlent de la peur que suscite une administration omnipotente. Ainsi dans l'intention de limiter le pouvoir de l'administration on la soumet à des obligations supplémentaires. En France, par exemple, la législation dispense les pouvoirs publics de l'obligation d'information parce qu'elle les soumet à une procédure plus contraignante qui est celle de l'autorisation⁴².

Ainsi la législation tunisienne encourage la mise sur pied des fichiers publics nominatifs "clandestins". Ils seront de plus en plus nombreux et tentaculaires, ils seront interconnectés et personne ne pourra savoir s'ils existent ou pas et où est-ce qu'ils sont localisés, quelle personne publique les gère et quelles données renferment-ils. On pourra même avancer que devant un juge les personnes publiques pourront nier l'existence de ces fichiers.

Avant de clore ces développements concernant l'obligation de publicité des fichiers, il est à révéler une incohérence de la loi de 2004. En effet, si la législation tunisienne n'oblige pas l'administration à informer de la mise sur pied des fichiers qu'elle utilise, comment est-ce que le public pourra demander d'y accéder ? Devant ce constat, il est légitime de se poser des questions sur le sens que peut revêtir l'article 55 qui dispose que "les personnes mentionnées à l'article 53 de la présente loi doivent rectifier, compléter, modifier, ou mettre à jour les fichiers dont elles disposent, ainsi que l'effacement des données à caractère personnel contenues dans ces fichiers...". Quelle est cette obligation qui est suspendue entre ciel et terre, sans aucune attache avec la réalité ? Car comment pourrait-on vérifier et même obliger l'administration au respect de ces règles, si on ne sait même pas que ces fichiers existent ?

Le même article continue pour déterminer dans quels cas l'administration est obligée de rectifier les données personnelles cachées, en disposant "... si la personne concernée, le tuteur ou les héritiers a signalé par n'importe quel moyen laissant une trace écrite, l'inexactitude ou l'insuffisance de ces données". Une construction pour le moins bizarre.

Mais les fichiers publics, même les plus dangereux pour le respect de la vie privée des individus, ne sont pas soumis pour leur création, contrairement à ceux privés, à la demande d'autorisation de l'Instance de contrôle.

⁴² Voir l'article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi du 6 août 2004. Celui-ci prévoit l'autorisation de création de ces fichiers soit par arrêté ministériel ou par décret pris en Conseil d'État. Dans tous les cas les actes de création sont pris après avis de la CNIL qui est annexé à l'acte et publié avec.

B. Des fichiers sans contrôle ou de la dispense d'autorisations de l'instance

L'exploitation de certains fichiers contenant des données à caractère personnel peut être attentatoire à la vie privée des individus. Ce danger est accru quand il s'agit de données que les législations comparées ont pris l'habitude de qualifier de "sensibles". Elles le sont car elles touchent à la nature même de la personne comme les données raciales ou génétiques parfois aux positions de l'individu comme les données concernant l'appartenance religieuse, politique ou syndicale enfin aux activités très personnelles comme les données concernant la santé ou la vie sexuelle. Les législations ont toujours commencé par en interdire en principe le traitement. Ensuite elles réglementent les exceptions possibles en prévoyant des conditions assez contraignantes pour le maître du fichier.

D'autres types de données sont assez "dangereuses" pour l'intimité des individus vivant en société. Ce sont ceux issues des caméras de surveillance placées dans les lieux publics et privés. En effet, ce genre de support permet de collecter une masse très importante d'informations sans que l'individu se rende compte parfois de l'existence même de ces capteurs. C'est pour cette raison que les législations se sont empressées de canaliser strictement leur utilisation.

L'article 8⁴³ de la loi tunisienne soumet ces traitements à une autorisation de l'Instance Nationale de protection des données personnelles. Ce sont principalement les traitements des données de l'article 14 portant sur les données sensibles ou de l'article 69⁴⁴ concernant les fichiers relatifs à la vidéo surveillance. L'Instance dans ce cas doit étudier le dossier et au vu des finalités déclarées du fichier peser le pour et le contre de la mise sur pied d'un tel fichier.

En effet, le traitement des informations dans des fichiers publics est dans tous les cas bénéfiques pour le citoyen. C'est à travers ces fichiers que les personnes publiques sont capables de mieux répartir leurs services entre les différentes régions du pays ou les différentes catégories sociales de la population. L'efficacité des missions dont sont chargées ces personnes passe nécessairement par le traitement d'une masse importante de données concernant les aspects les plus intimes des personnes. Pour ne prendre qu'un exemple, comment est-ce que les autorités sanitaires chargées de la salubrité publique peuvent-elles être efficaces, si elles ne peuvent gérer des fichiers contenant des informations sur les épidémies saisonnières comme la grippe ou l'angine ou alors le choléra ? Ce fichier qui collecte toutes les alertes données par les professionnels de santé ne peut aboutir aux finalités escomptées,

⁴³ L'article 8 de la loi tunisienne dispose que : "Dans les cas où la présente loi exige l'obtention d'une autorisation de l'Instance pour le traitement des données à caractère personnel, la demande d'autorisation doit comprendre notamment les informations suivantes ..."

⁴⁴ L'article 69 de la loi tunisienne dispose que : "Sous réserve de la législation en vigueur, l'utilisation des moyens de vidéosurveillance est soumise à une autorisation préalable de l'Instance Nationale de Protection des Données à Caractère Personnel ...".

s'il ne rassemble pas des informations personnelles sur les malades tel que leur sexe, âge ou localisation, origine sociale ou activité professionnelle.

C'est pour ces besoins d'efficacité que les législations comparées ont permis sous certaines conditions, plus spécialement aux personnes publiques, de traiter ces données. Mais ces exceptions au principe général d'interdiction sont entourées de garanties pour protéger la vie privée des individus.

En Tunisie, l'article 54 déclare que les personnes publiques ne sont pas soumises à l'obligation de l'article 8 de la loi 2004-63. Ainsi, elles ne sont donc pas tenues de demander l'autorisation de l'Instance de contrôle, même quand il s'agit de la mise sur pied de fichiers aussi dangereux pour la vie privée des citoyens.

Cette situation s'avère unique en droit comparé. En effet, les législateurs étrangers, partant du constat que les fichiers publics, plus que les fichiers privés, sont plus à même de porter atteinte à la vie privée des individus, ont soumis leur création à des procédures plus contraignantes. Celles-ci permettent de mieux sauvegarder les droits des individus contre un État "potentiellement Léviathan".

Le meilleur exemple à ce propos est indubitablement l'article 25 nouveau de la loi française. Celui-ci pose comme principe que certains fichiers sont soumis à la procédure de l'autorisation. Il en dénombre huit, qui sont de par leur contenu, des fichiers potentiellement dangereux pour la préservation de l'intimité de l'individu. Ce sont les traitements qui portent sur des données statistiques, des données à caractère politique, philosophique ou justifiées par un intérêt public, des données génétiques, des données relatives aux infractions, condamnations et mesures de sûreté, permettant l'interconnexion de fichiers de personnes morales gérant un service public, comportant l'identifiant unique qui est le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, des données comportant une appréciation sur les difficultés sociales des personnes ou enfin des données biométriques nécessaires au contrôle de l'identité des personnes.

Ceux sont là d'ailleurs des données ou des traitements qui, de par leur nature, sont normalement du ressort des personnes publiques. Mais le même article exclut dans son chapeau les grands fichiers détenus par les personnes publiques puisqu'il dispose que "sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 ...". Ces deux dispositions concernent les fichiers détenus par les personnes publiques comme ceux relatifs à la sûreté de l'État, la défense ou la sécurité publique, aux infractions pénales, à l'utilisation dans les fichiers publics du numéro d'identification nationale, des recensements ainsi que les téléservices ... Le lecteur peut de prime abord croire que ces fichiers publics sont exonérés de cette obligation d'obtenir l'autorisation, mais il doit réviser très rapidement son jugement à la lecture des articles en question.

En France, quand l'administration déroge au principe de l'autorisation de la CNIL, la loi prévoit d'autres conditions de nature à préserver les droits des individus et

sans complètement évacuer la structure de contrôle. En effet, l'article 26 de la loi française autorise les fichiers publics relatifs à certains domaines mais "... par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés ... l'avis de la commission est publié avec l'arrêté autorisant le traitement"⁴⁵. Concernant le traitement des données sensibles, leur traitement par les personnes publiques doit être autorisé par "décret en Conseil d'État pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement"⁴⁶. La loi va même jusqu'à permettre la dispense de publication des décrets cités plus haut à condition qu'"... est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission"⁴⁷.

On remarque que si les personnes publiques peuvent dans des secteurs définis déroger au principe de l'autorisation préalable de la CNIL, elles sont soumises à une autre procédure d'autorisation garantissant la publication dans tous les cas de l'avis de la CNIL. Ainsi la structure de contrôle n'est pas évacuée, au contraire, son avis indépendamment de la décision prise par les pouvoirs publics est rendu public. Dans cette situation, c'est l'opinion publique qui en tirera les conséquences qui s'imposent.

D'autres exemples pris du droit comparé peuvent être avancés et montrer clairement que vis-à-vis des fichiers publics, la position est d'augmenter les obligations à la charge des personnes publiques, et non pas de les diminuer. C'est ainsi qu'en Italie, il est nécessaire d'obtenir une loi d'autorisation⁴⁸ pour que les personnes publiques puissent mettre sur pied des fichiers traitant des données à caractère personnel. Le Luxembourg quant à lui a prévu une autorisation réglementaire pour la mise sur pied des fichiers publics les plus importants et concernant le traitement des infractions et des peines et relatifs à la sécurité publique à la défense nationale et à la sûreté de l'État. Dans ces cas, la loi prévoit des pouvoirs accrus de contrôle sur le

⁴⁵ Article 26 I de la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004.

⁴⁶ Article 26 II de la loi française du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés.

⁴⁷ *ibidem*.

⁴⁸ Voir la section 20 du code de protection des données personnelles italien du 30 juin 2003, intitulée Principles Applying to the Processing of Sensitive Data qui dispose que "1. Processing of sensitive data by public bodies shall only be allowed where it is expressly authorised by a law specifying the categories of data that may be processed and the categories of operation that may be performed as well as the substantial public interest pursued ... 3. If the processing is not provided for expressly by a law, public bodies may request the Garante to determine the activities that pursue a substantial public interest among those they are required to discharge under the law. Processing of sensitive data shall be authorised in pursuance of Section 26 (2) with regard to said activities, however it shall only be allowed if the public bodies also specify and make public the categories of data and operation in the manner described in paragraph 2".

contenu des fichiers et des possibilités d'accès, c'est vrai indirects, mais avec de possibles communication et radiation des données⁴⁹.

Ainsi, les personnes publiques ne sont pas dispensées de l'obligation d'obtenir des autorisations préalables, au contraire elles sont soumises à des procédures plus contraignantes leur permettant de mettre sur pied des fichiers contenant des données à caractère personnel.

Il faut enfin signaler que les législations comparées n'ont généralement pas réservées des dispositions particulières au traitement des données personnelles issues des systèmes de vidéosurveillance⁵⁰. Ceci s'explique par le fait qu'ils ont réservés une loi particulière au traitement des données issues de ce mode de surveillance. La France, par exemple, réserve la loi d'orientation et de programmation relative à la sécurité, à gérer ce genre de données⁵¹. Les personnes publiques sont soumises aussi à des autorisations et prévoit des garanties pour les citoyens permettant de préserver ainsi la vie privée des citoyens.

⁴⁹ Voir l'article 17 de la loi luxembourgeoise du 2 août 2002 qui est intitulé autorisation par voie réglementaire et qui dispose que "(1) Font l'objet d'un règlement grand-ducal : (a) les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés ... (b) les traitements relatifs à la sûreté de l'État, à la défense et à la sécurité publique, et (c) les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol).

(2) Le contrôle et la surveillance des traitements mis en œuvre tant en application d'une disposition de droit interne qu'en application d'une convention internationale est exercé par une autorité de contrôle composée du Procureur Général d'État, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre.

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission. Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées ci-dessus. L'autorité de contrôle fait opérer les rectifications et radiations nécessaires. Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution ...". Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, Journal Officiel du Grand-duché de Luxembourg, recueil de législation n° 91 du 13 août 2002

⁵⁰ Voir de plus amples développements *infra* II.D.

⁵¹ Voir la loi n° 95-73 du 21 janvier 1995 intitulée loi d'orientation et de programmation relative à la sécurité, publié au *Journal officiel de la république française* le 24 janvier 1995, telle que modifiée à plusieurs reprises et dernièrement par la loi n° 200-204 en date du 9 mars 2004 publiée au *JORF* le 10 mars 2004. Texte disponible dans sa version mise à jour sur le site www.legifrance.gouv.fr

Le législateur tunisien est allé plus loin dans la dispense de l'administration de l'obtention de n'importe quelle autorisation de l'Instance. En effet, l'article 49⁵² de la loi dispose que "les données à caractère personnel traitées pour des finalités particulières peuvent être communiquées en vue d'être traitées une autre fois pour des fins historiques ou scientifiques, à condition d'obtenir le consentement de la personne concernée, de ses héritiers ou de son tuteur, ainsi que l'autorisation de l'Instance Nationale de Protection des Données à Caractère Personnel". Ainsi toute communication des données à des fins spécifiques est soumise, en plus du consentement de la personne, à l'autorisation de l'Instance. Cette précaution est prise afin d'éviter que le maître d'un fichier ne contourne la procédure préalable de mise sur pied de fichiers (demande d'autorisation ou de déclaration) en collectant les données non pas directement chez les personnes intéressées mais à travers d'autres fichiers déjà constitués.

L'article 54 de la loi de 2004 exonère les personnes publiques encore une fois de l'autorisation de l'Instance de contrôle. Ainsi rien n'interdira que les personnes publiques collectent les données personnelles sur les individus là où elles sont stockées dans des systèmes informatiques de personnes tierces autorisées à traiter ces données. Tous les fichiers privés et publics peuvent de ce fait alimenter les fichiers publics en données personnelles, les fichiers des banques, des assurances, des médecins, des hôtels, des sociétés de transport, des sociétés commerciales ... De cette façon, la loi démontre que dans la conception même de la chose publique par les pouvoirs publics, il est inadmissible de soumettre l'administration à un contrôle quelconque.

Dans ce cas de figure, la personne publique, maîtresse du fichier, est dispensée d'obtenir l'autorisation de l'Instance ainsi que le consentement des personnes concernées. Consentement dont sont dispensés de manière générale, les personnes publiques comme il sera exposé dans ce qui suit.

C. Des fichiers imposés ou de la dispense d'obtention du consentement

La collecte des données personnelles doit impérativement passer par l'obtention du consentement des personnes concernées. C'est là une règle de principe que l'on retrouve clairement transcrite aussi bien dans toutes les législations nationales que dans les textes internationaux. Mais avant d'étudier la soumission des personnes publiques à cette condition commençons par chercher quel sens donner au consen-

⁵² L'article 49 de la loi de 2004 dispose que "les données à caractère personnel traitées pour des finalités particulières peuvent être communiquées en vue d'être traitées une autre fois pour des fins historiques ou scientifiques, à condition d'obtenir le consentement de la personne concernée, de ses héritiers ou de son tuteur, ainsi que l'autorisation de l'Instance Nationale de Protection des Données à Caractère Personnel ...".

tement ? Qu'elles en sont les conditions ? Comment est traité le consentement dans la loi tunisienne ?

Malgré le fait que le consentement constitue le titre de la sous-section une de la section trois traitant des droits des personnes concernées, l'article 6 de la loi tunisienne ne définit pas cette notion. Par contre la loi luxembourgeoise du 2 août 2002 qui ne fait que reprendre l'article 2 h de la directive européenne⁵³ stipule en son article 2 que c'est "toute manifestation de volonté ... par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement". C'est ainsi que l'approbation par la personne concernée de divulguer les données personnelles la concernant en vue d'être traitées par le responsable du fichier. L'importance du consentement apparaît dans sa consécration par la charte des droits fondamentaux de l'union européenne stipule dans son article 8 que "ces données doivent être traitées ... sur la base du consentement de la personne concernée ...". Le principe du consentement préalable à la collecte et au traitement des données a été déclaré par la cour constitutionnelle allemande en décembre 1983 comme de valeur constitutionnelle dans le cadre du "droit d'autodétermination informationnelle"⁵⁴. Un droit qui habiliterait tout individu à "disposer" de manière libre et souveraine des informations qui se rapportent à sa personne.

Aussi bien dans la loi tunisienne que dans les législations comparées⁵⁵, le consentement revêt des conditions de validité. En synthétisant ces conditions, on dira que celui-ci doit être informé⁵⁶, libre⁵⁷, express⁵⁸, non équivoque⁵⁹, indubitable⁶⁰ et dans certaines législations écrit⁶¹.

⁵³ L'article 2 de la directive du Conseil de l'Europe adopté le 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnels, stipule : "Définitions : Aux fins de la présente directive, on entend par : ... h) "consentement de la personne concernée" : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement". P.E. et C.E., JOCE 23 novembre 1995, n° 1, 281.

⁵⁴ Cité dans le livre blanc, *administration électronique et protection des données personnelles*, dénommé rapport Truche mais dont les auteurs sont au nombre de trois : Truche (P.), Faugère (J-P.), Flichy (P.), Ministère de la fonction publique, la documentation française, Paris, février 2002, p. 17.

⁵⁵ Article 7 de la directive du Conseil de l'Europe, *idem* : "Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si : a) la personne concernée a indubitablement donné son consentement ..." et les lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel adoptée le 23 septembre 1980. "Principe de la limitation en matière de collecte. 7. Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement".

⁵⁶ L'article 4a de la loi allemande stipule à propos de la personne concernée que : "... Celle-ci est à informer de la finalité prévue de la collecte, du traitement ou de l'utilisation, ainsi que, dans la mesure où les circonstances du cas particulier l'exigent, ou sur sa demande, des conséquences d'un refus du consentement ...".

Il est tout à fait normal que la personne concernée ne puisse donner son consentement que si elle a été préalablement informée de toute les données pouvant l'éclairer sur le sort des données recueillies ainsi que des droits dont il peut profiter. Ainsi l'article 31 de la loi tunisienne pose la condition que cette information doit se faire par n'importe quel moyen laissant une trace écrite et doit être préalable à l'opération de collecte. Le maître du fichier doit exposer la nature des données et la finalité du traitement mais surtout informer la personne du caractère facultatif ou obligatoire de donner ces informations. La personne concernée est à cette occasion, d'après la même disposition, informée de l'identité du maître du fichier, de son droit d'accès, de son droit possible d'opposition, de sa possible rétractation ainsi que de la durée de conservation des données. Toute une série d'informations qui sont de nature à éclairer le citoyen, avant qu'il ne donne son consentement à cette opération, le plaçant dans une position lui permettant de juger s'il a intérêt ou pas de concéder ce droit au maître du fichier. Approbation qui peut être, d'après l'article 27 paragraphe 2, retirée à n'importe quel moment.

L'accord donné par la personne concernée doit être clair et non équivoque et ne peut de ce fait être présumé ce qui a d'ailleurs été rejeté aussi bien par les législations comparées que par la doctrine. La directive européenne de 1995 parle du caractère indubitable du consentement dans son article 7. Un qualificatif excluant tout doute possible et rendant l'accord donné incontestable. Une condition qui a été indirectement prévue par la loi en spécifiant qu'il devait être écrit. Ce qui le rend indubitable et incontestable, mais pose certains problèmes pratiques. En effet, si dans la plupart des cas on présente un formulaire à remplir aux personnes concernées, la collecte des données peut être aujourd'hui réalisée par d'autres canaux. Sur le réseau Internet, il paraît difficile de demander l'écrit dans le cadre de transactions immédiates et immatérielles. Les législations étrangères ont prévu des dispositions spécifiques pour la protection des données à caractère personnel sur le réseau In-

⁵⁷ L'article 11 de la loi italienne stipule que "... Le consentement n'est valablement donné que s'il est exprimé librement ...". La loi autrichienne dans la section de définition des termes utilisés réserve le point 14 pour définir le consentement comme "the valid declaration of intention of the data subject, given without constraint". C'est ainsi un consentement sans contrainte. La loi de Bosnie Herzégovine stipule aussi à ce propos que : "the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

⁵⁸ La loi australienne stipule que "consent means express consent or implied consent".

⁵⁹ La loi luxembourgeoise déclare que le consentement de la personne concernée est "toute manifestation de volonté expresse, non équivoque".

⁶⁰ La loi belge dispose en son article 5 que "Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants : a) lorsque la personne concernée a indubitablement donné son consentement; ...".

⁶¹ La loi argentine stipule dans ce sens "... 1.- The treatment of personal data is unlawful when the data owner has not given his or her express consent, which must be given in writing, or through any other similar means, depending on the circumstances ...".

ternet ou une possibilité d'interprétation conforme au monde virtuel⁶², ce que la loi tunisienne a omis de faire⁶³.

Mais les législations comparées prévoient des exceptions à cette obligation d'obtention préalable du consentement de la personne concernée. Ainsi la loi française, pour ne prendre que cet exemple, permet de se passer du consentement dans cinq cas que l'article 7 détaille⁶⁴. L'article 29 de la loi tunisienne a été d'ailleurs rédigé dans le même sens⁶⁵ sans prévoir le troisième cas prévu par la loi française relatif à la mission de service public. En effet, la loi dispense de l'obtention du consentement de la personne concernée, lors de la collecte des données à caractère personnel, quand cette opération est réalisée dans le cadre de "l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement". Il est évident que c'est au juge en dernier ressort de déterminer pour chaque cas est-ce que le responsable du traitement agit bien dans le cadre de l'exécution d'une mission de service public.

La loi organique tunisienne, a par contre en un seul article écarté cette obligation pour toutes les personnes publiques tels que définies dans l'article 53. Chaque fois qu'il s'agit pour le titulaire du traitement d'obtenir le consentement soit de la personne concernée soit de son tuteur, elle en dispense l'administration publique. L'article 54⁶⁶ est à ce sujet assez clair, les administrations citées ne sont pas soumises aux trois obligations suivantes : l'obligation d'obtenir le consentement de la

⁶² L'article 4 de la loi fédérale du premier janvier 2002 en Allemagne dispose que : "... Le consentement doit être donné par écrit, sauf si des circonstances particulières rendent une autre forme plus appropriée ...".

⁶³ Voir directive 2002/58/CE du Parlement et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques en date du 12 juillet 2002, sur le site de l'Union européenne à l'adresse www.europa.eu.int/eur-lex/pri/fr/oj/dat/2002/l_201/l_2012002073lfr00370047.pdf

⁶⁴ L'article 7 de la loi française de 1978 telle que révisée en 2004 dispose qu'"un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : 1° Le respect d'une obligation légale incombant au responsable du traitement ; 2° La sauvegarde de la vie de la personne concernée ; 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ; 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée".

⁶⁵ L'article 29 de la loi organique de 2004 dispose que : "Le traitement des données à caractère personnel n'est pas soumis au consentement de la personne concernée lorsqu'il s'avère manifestement que ce traitement est effectué dans son intérêt et que son contact se révèle impossible, ou lorsque l'obtention de son consentement implique des efforts disproportionnés, ou si le traitement des données à caractère personnel est prévu par la loi ou une convention dans laquelle la personne concernée est partie".

⁶⁶ L'article 54 de la loi organique tunisienne stipule bien que "Le traitement réalisé par les personnes mentionnées à l'article précédent n'est pas soumis aux dispositions prévues par les articles ... 27, 28 ... 44 de la présente loi".

personne concernée (article 27), l'obligation d'obtenir le consentement du tuteur et de l'autorisation du juge des mineurs (article 28⁶⁷) et l'obligation d'obtenir le consentement de la personne concernée si on a l'intention de collecter les données auprès des tiers (article 44)⁶⁸.

Ainsi les personnes publiques en droit tunisien sont dispensées sans aucune condition ni limite de l'obtention du consentement de la personne concernée indépendamment de la finalité du traitement. Qu'il s'agisse de mission de service public ou d'activité commerciale et en toute impunité à l'abri de tout contrôle, ces personnes peuvent récolter ces informations sans information préalable et sans attendre le consentement des personnes concernées. Plus que cela, elles peuvent récolter ces données à caractère personnel chez les tiers sans obtenir le consentement de ces personnes. Ainsi, toutes les données auxquelles le citoyen bien informé aurait consenti la collecte auprès des personnes privées telle que les banques ou d'une manière générale les sociétés commerciales, peuvent alimenter les bases de données des personnes publiques. Une carte blanche pour les personnes publiques, pour l'administration, de nature à mettre en péril la vie privée des individus.

Ces personnes publiques sont même autorisées par la loi, à traiter les données relatives aux infractions et poursuites pénales sans aucune limite.

D. Des fichiers sans limite ou de la dispense de l'interdiction de traiter des données relatives aux infractions et aux poursuites pénales

Le traitement des données relatives aux infractions, des condamnations ou des mesures de sûreté est interdit par la plupart des textes nationaux. La loi tunisienne de 2004 ne déroge pas à ce principe, c'est ainsi qu'elle dispose en son article 13 qu'"est interdit le traitement des données à caractère personnel relatives aux infractions, à leur constatation, aux poursuites pénales, aux peines, aux mesures préventives ou aux antécédents judiciaires". C'est là une déclaration de principe.

Mais du fait que ces données, comme toute les autres, doivent bien être traitées quelque part dans la société, toutes les législations prévoient des dérogations possibles à ce principe. Ces exceptions permettent principalement d'éviter que des personnes privées ne gèrent sans contrôle ce genre de données et même, quand l'autorité publique est emmené à le faire, cette opération doit être entourée des ga-

⁶⁷ L'article 28 de la loi organique tunisienne stipule que "Le traitement des données à caractère personnel qui concerne un enfant ne peut s'effectuer qu'après l'obtention du consentement de son tuteur et de l'autorisation du juge de la famille [qui] peut, à tout moment, revenir sur son autorisation".

⁶⁸ La loi fédérale allemande du 1^{er} janvier 2002, dans son article 13 paragraphe 1a, prévoit le cas de la collecte par les organismes publics auprès des tiers de données à caractère personnel. Elle prévoit l'autorisation éclairée du tiers en disposant que : "Lorsque des données à caractère personnel sont collectées auprès d'un organisme privé au lieu d'être collectées auprès de la personne concernée, il faut informer cet organisme de la disposition légale rendant ces renseignements obligatoires ou, le cas échéant, du caractère facultatif de ces renseignements".

ranties permettant de préserver la vie privée des individus. C'est dans ce sens que la directive européenne 95/46 stipule que "le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique"⁶⁹.

Ainsi, on constate que dans les législations européennes ayant intégré cette directive, le traitement de ces données est normalement interdit pour la grande majorité des personnes privées. Par contre celles qui sont emmenés à traiter dans leurs activités ces informations, par exemple les avocats ou d'une manière générale les auxiliaires de justice⁷⁰, ils ne peuvent le réaliser que sous certaines conditions. Certaines catégories de personnes publiques gèrent dans le cadre de leurs missions les enquêtes judiciaires et veillent à l'application des peines prononcées par les juridictions nationales, il est donc tout à fait normal de les soustraire à cette interdiction. Par contre, des garanties appropriées et spécifiques doivent être prévues. La plus importante protection pour les citoyens est celle de rendre public cette catégorie de fichiers par le biais de la déclaration dont est tenu le maître du fichier et de le soumettre aux inspections de la structure de contrôle. Une garantie écartée par la loi tunisienne comme traité *supra*⁷¹.

Mais même en dehors de ces garanties minimales, les législations comparées, dressent des limites à la mise sur pied de cette catégorie de fichiers. Par exemple en dénombrant limitativement les personnes publiques habilitées à le faire. C'est ainsi que la loi sur la protection des données de la principauté de Monaco réserve le traitement de ces données aux autorités judiciaires et administratives⁷². C'est aussi le cas de la loi française après sa révision de 2004 qui stipule en son article 9 que "les

⁶⁹ Article 8 paragraphe 5 de la directive du Conseil de l'Europe adoptée le 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnels, P.E. et C.E., JOCE 23 novembre 1995, n° 1, 281.

⁷⁰ Voir l'article 9 de la loi française qui dispose que : "les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par : ... 2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ...".

⁷¹ Voir développements *supra* I.A. et B.

⁷² L'article 11 de la loi 1.165 réglementant le traitement d'informations nominatives du 23 décembre 1993 de la Principauté de Monaco stipule que "nul ne peut procéder à des opérations de collecte, d'enregistrement ou d'utilisation d'informations nominatives à caractère médical ou concernant des infractions, des condamnations ou des mesures de sûreté.

Toutefois, peuvent procéder à de telles opérations, dans le cadre exclusif des missions qui leur sont légalement conférées : 1° les autorités judiciaires et les autorités administratives pour ce qui est des informations nominatives concernant des infractions, des condamnations ou des mesures de sûreté ..."

traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par : 1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ...”. Mais la loi française soumet ce genre de traitement soit à l’autorisation préalable de la CNIL soit à celle du Ministre compétent après avis de la CNIL⁷³.

D’autres législations prévoient qu’un texte spécifique fixera les modalités de cette dérogation. C’est le cas de la loi belge qui commence par interdire dans son article 8 §1 le traitement de ce genre de données⁷⁴. Mais elle réserve les paragraphes suivants à prévoir les dérogations possibles ainsi que les modalités de leur application. Le paragraphe le plus important est qu’un texte fixera les modalités d’application de cette dérogation⁷⁵. Celui-ci est pris après avis de la structure de contrôle.

La loi organique tunisienne écarte simplement cette interdiction par rapport aux personnes publiques de l’article 53. En effet l’article 54 permet à toutes ces personnes publiques, aussi bien les “autorités publiques” que les collectivités territoriales que les établissements publics administratifs mais aussi celles du paragraphe deuxième qui sont les établissements publics de santé et les établissements publics non administratifs, de mettre sur pied des fichiers contenant ces données sans aucune garantie pour les citoyens. Aucune obligation n’est prévue à ce sujet.

Ainsi les personnes publiques d’après les dispositions de l’article 53 et quelque soit leur mission, pourront traiter les données à caractère personnel relatives aux citoyens en “cachette”. Quand, pour certaines catégories de données, les personnes privées sont soumises à une demande d’autorisation préalable, les personnes publiques en sont dispensées. Quand on fait de l’obligation d’obtenir pour le maître du fichier le consentement du citoyen préalablement à la collecte et au traitement un principe général, en on dispense les personnes publiques. Et même pour les données plus “délicates” comme c’est le cas de celles relatives aux infractions et aux

⁷³ Article 25-I-33 et 26-I-2 de la loi française du 6 janvier 1978.

⁷⁴ Article 8 de la loi belge : “§ 1. Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu’aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté est interdit ...”.

⁷⁵ Article 8 de la loi belge : “... § 2. L’interdiction de traiter les données à caractère personnel visées au § 1er n’est pas applicable aux traitements effectués : (a) sous le contrôle d’une autorité publique ou d’un officier ministériel au sens du Code judiciaire, lorsque le traitement est nécessaire à l’exercice de leurs tâches ; (b) par d’autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d’une loi, d’un décret ou d’une ordonnance ; (c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l’exige ; (d) par des avocats ou d’autres conseils juridiques, pour autant que la défense de leurs clients l’exige ; (e) pour les nécessités de la recherche scientifique, dans le respect des conditions fixées par le Roi par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée. § 4. Le Roi fixe par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, les conditions particulières auxquelles doit satisfaire le traitement des données à caractère personnel visées au § 1”.

poursuites pénales, on pose le principe de l'interdiction de leur traitement, mais on donne "carte blanche" pour les personnes publiques pour le faire, sans aucune limite ni garantie.

Ainsi l'administration publique dans son sens le plus large bénéficie d'un régime dérogatoire généralisé. Elle peut traiter comme elle le désire les données personnelles des administrés sans leur donner aucun moyen de préserver leur vie privée. Mais la loi organique tunisienne ne s'arrête pas à ce niveau, elle va plus loin. En effet, ce que l'on vient de traiter concernent toutes les personnes publiques telles que définies dans l'article 53, mais la première catégorie de ces personnes publiques (autorités publiques, collectivités publiques, établissements publics administratifs) vont profiter d'encore plus de latitude pour collecter et traiter des données à caractère personnel plus sensibles.

II. DES FICHIERS PUBLICS POUVANT TRAITER LES DONNÉES SENSIBLES ET DE VIDEOSURVEILLANCE SANS LIMITATION AUCUNE

Les personnes publiques de la première catégorie de structures ne sont pas soumises au régime très contraignant que la loi organique de 2004 a établie relativement aux données dites sensibles et celles collectées à travers les moyens de vidéo surveillance. On peut effectivement lire dans cette disposition que "le traitement réalisé par les personnes mentionnées au premier paragraphe de l'article 53 de la présente loi n'est pas soumis également aux dispositions des articles 14, 15 et 42 et aux dispositions de la quatrième section du cinquième chapitre de la présente loi", section relative à la vidéo surveillance.

Ainsi cette disposition, par un seul alinéa, fait bénéficier les personnes publiques citées et quelque soit la mission qu'elles assument de la possibilité de traiter les données sensibles (A), en excluant le droit d'opposition des individus (B), ainsi que leur droit d'accès (C). Enfin ces personnes publiques ne sont pas entravées dans leurs missions par les règles de droit commun régissant le traitement des données collectées par les moyens de vidéosurveillance (D).

A. Des fichiers publics autorisés à traiter sans limite les données sensibles

Les législations comparées font bénéficier certaines données d'un régime spécifique restreignant en cela les droits des personnes autorisées à les traiter. Ce régime spécifique s'explique par le fait que ces informations sont de nature à ouvrir la voie à des grandes discriminations entre les individus. Ces informations personnelles sont généralement dénommées "données sensibles". La loi tunisienne, sans leur donner ce qualificatif, en traite dans l'article 14 en déclarant qu'elles "... concernent, directement ou indirectement, l'origine raciale ou génétique, les convictions religieuses, les opinions politiques, philosophiques ou syndicales, ou la santé". Les

différentes législations étudiées élargissent ou restreignent cette énumération. Ce qui a emmené l'OCDE à relever que les législations nationales divergent quant à la définition de cette catégorie de donnée⁷⁶. En comparant ces législations⁷⁷ avec la loi organique tunisienne on remarque que la différence principale entre elles réside dans l'omission de la loi organique de 2004 d'une catégorie de donnée, c'est celle relative à la vie sexuelle des individus. On ne voit à cela qu'une seule explication plausible : le législateur n'a pu inclure ce genre de données car probablement la culture arabo-musulmane est peu encline à dissenter de ces choses, sauf si le législateur a considéré que la vie sexuelle faisait partie de la santé des individus ! Ce serait là matière à discussion.

⁷⁶ Voir le point 6 de l'exposé des motifs des lignes directrices de l'OCDE qui déclare à ce propos que : "6. Les différences entre les démarches nationales, telles qu'elles se dégagent à l'heure actuelle des lois, projets de lois ou propositions de législation, concernent des aspects tels que la portée de la législation, l'importance accordée à divers éléments de la protection, les modalités détaillées de mise en oeuvre des principes généraux susmentionnés et le mécanisme d'application ... On constate que les catégories de données sensibles sont définies de façon différente ..." et plus loin de déclarer qu'"en fait, il n'est probablement pas possible de définir un ensemble de données qui soient universellement considérées comme sensibles".

⁷⁷ Voir la *personal data protection act* d'Argentine en date du 4 octobre 2000 qui définit dans sa section 2 les *sensitive data* de la façon suivante : "Personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior". Voir une définition plus détaillée donnée par la *privacy act* australienne n° 119 de 1988 telle qu'amendé en 2005 suivant laquelle les *sensitive data* sont : "(a) information or an opinion about an individual's : (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual". Voir la loi chypriote n° 138 intitulée *the processing of personal data* date de 2001 qui dans son point 2 réserve aux définitions inclus dans les données sensibles les orientations érotiques en stipulant que cette catégorie de données comprend les : "data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in a body, association and trade union, health, sex life and erotic orientation as well as data relevant to criminal prosecutions or convictions". La loi estonienne y intègre entre autre les données génétiques en déclarant dans sa *personal data protection act* datant du 12 février 2003 dans son paragraphe 4 que les *sensitive data* sont : "1) data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law; 2) data revealing ethnic or racial origin; 3) data relating to the state of health or disability; 4) data relating to genetic information; 5) data relating to sexual life; 6) data concerning membership in trade unions; 7) information collected in criminal proceedings or in other proceedings to ascertain an offence before a public court session or before a judgment is made in a matter concerning an offence, or if this is necessary in order to protect public morality or the family and private life of persons, or where the interests of a minor, a victim, a witness or justice so require". La loi fédérale allemande de protection des données du 1er janvier 2002, dans son article 3 point 9, dénomme ces données comme "catégorie spéciale de données à caractère personnel" et les définit comme "... toutes les informations relatives à l'origine raciale et ethnique d'une personne, à ses opinions politiques, ses convictions religieuses ou philosophiques, son appartenance syndicale, sa santé ou sa vie sexuelle".

Après avoir réalisé cette opération de définition, les législations aussi bien internationales que nationales énoncent clairement le principe de l'interdiction de traitement des données sensibles⁷⁸ se conformant en cela les lignes directrices des Nations Unies⁷⁹. La loi tunisienne ne déroge pas à cette position unanime. Dans l'article 14 la loi organique pose le principe concernant les données sensibles : l'interdiction de les traiter. En effet, la disposition déclare qu'il : "Est interdit le traitement des données à caractère personnel qui concernent ..." et de les énumérer comme expliqué *supra*.

Mais même les lignes directrices des Nations Unies⁸⁰ comme c'est le cas de celles de l'OCDE⁸¹ réservent une disposition prévoyant la possibilité pour les législations nationales d'établir des exceptions à cette interdiction. La convention européenne pour la protection des personnes contre le traitement automatisé des données à caractère personnel du 28 janvier 1981 disposait déjà dans son article 6 que "les don-

⁷⁸ Voir la loi portugaise du 26 octobre 1998 qui stipule dans son article 7 que "1. Le traitement de données à caractère personnel qui révèlent ... sont interdits". Voir la loi française et plus spécialement l'article 8 qui stipule que "I. Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement ...". Voir également l'article 7 de la loi hellénique 2472/1997 de 1997 telle qu'amendée en 2001 qui dispose que : "1. The collection and processing of sensitive data is prohibited". Voir dans le même sens la loi argentine qui dispose en sa section 7 que "3.- It is prohibited to create files, banks or registers storing information that directly or indirectly reveals sensitive data". Voir la loi chypriote qui dans son point 6 stipule que : "6. (1) The collection and processing of sensitive data is prohibited".

⁷⁹ La résolution des Nations Unies réserve son point cinq pour traiter des données sensibles. On peut y lire en effet que "sous réserve des cas de dérogations limitativement prévus sous le principe 6, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées".

⁸⁰ La même résolution des Nations Unies réserve son point six pour traiter des dérogations possibles entre autre à l'interdiction du traitement données sensibles. On peut y lire en effet que "des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées. Les dérogations au principe 5 relatif à la prohibition de la discrimination, outre qu'elles devraient être soumises aux mêmes garanties que celles prévues pour les dérogations aux principes 1 à 4, ne pourraient être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits de l'homme et de la lutte contre les discriminations".

⁸¹ Les lignes directrices de l'OCDE dans le point 34 de ses visas déclare à ce propos que : "considérant que les États membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale -particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie- et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes".

nées à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées ...". Ces dérogations s'expliquent par le fait qu'il est indispensable dans nos sociétés modernes de traiter les données sensibles malgré leur "dangerosité" potentielle. Mais les lignes directrices imposent dans ce cas aux législations nationales de prendre les mesures nécessaires pour limiter ces dérogations et surtout les entourer des "garanties appropriées" de nature à éviter tout traitement entraînant des ségrégations entre les citoyens. Les lignes directrices des Nations Unies vont plus loin puisqu'elles considèrent que les dérogations prévues par les États doivent être conformes avec les règles édictées dans la charte internationale des droits de l'homme et tous les "textes luttant contre les discriminations".

Toutes les législations comparées prévoient ainsi des exceptions à cette interdiction qu'elles soumettent à des règles strictes comme celle d'obtenir l'accord exprès et écrit des personnes concernées qui est généralement cumulé avec l'obtention d'une autorisation préalable de la part de l'autorité de contrôle. La convention européenne pour la protection des personnes contre le traitement de ces données stipule que ces dérogations doivent rentrer dans le cadre des "mesures nécessaires dans une société démocratique"⁸².

C'est ainsi que le paragraphe deuxième de l'article 14 de la loi organique tunisienne synthétise ces dérogations prévues en droit comparé. Le texte limite ainsi le traitement des données sensibles aux quatre situations suivantes en disposant que cela est permis "... lorsqu'il est effectué avec le consentement exprès de la personne concernée donné par n'importe quel moyen laissant une trace écrite, ou lorsque ces données ont acquis un aspect manifestement public, ou lorsque ce traitement s'avère nécessaire à des fins historiques ou scientifiques, ou lorsque ce traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée". Il est à noter qu'en ce qui concerne les données relatives à la santé, la loi organique a réservé toute une section du chapitre cinq pour en réglementer le traitement. Cette disposition traite des dérogations de manière générale indépendamment de la qualité des personnes qui vont entreprendre le traitement de cette catégorie de données.

On remarque à ce propos que les législations nationales prévoient des exceptions spécifiques au principe de l'interdiction concernant les personnes publiques en po-

⁸² La convention européenne pour la protection des personnes contre le traitement automatisé des données à caractère personnel du 28 janvier 1981 dispose dans son article 9.2 qu'"Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique : a. à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ...".

sant des conditions draconiennes pour les en faire bénéficiaire⁸³. C'est ainsi qu'en Italie la loi exclue des personnes publiques les établissements publics économiques et dispose qu'il doit être "autorisé par une expresse disposition de loi spécifiant les données pouvant être traitées, les opérations pouvant être effectuées et les motifs d'intérêt public importants qui sont poursuivis". Au Portugal cela n'est possible que par "disposition légale ou autorisation de la CNPD [autorité de contrôle portugaise], ... pour des motifs d'intérêt public important, [et lorsqu'] il est indispensable à l'exercice des fonctions légales ou statutaires de son responsable". Ainsi, les personnes publiques ne profitent pas d'une dispense générale, il faut d'ailleurs garder à l'esprit que ces personnes sont soumises aux règles de protection édictées dans les lois nationales comme traitées *supra*.

Ce n'est pas le cas de la loi tunisienne qui après avoir régi le traitement des données sensibles conformément aux lignes directrices aussi bien des Nations Unies que de l'OCDE, soustrait encore une fois, les personnes publiques énoncées au pa-

⁸³ Voir la loi italienne, plus spécialement l'article 22 qui stipule que "1. Les données à caractère personnel ... ne peuvent faire l'objet d'un traitement qu'avec le consentement écrit de la personne concernée et après autorisation du *Garante* ... 3. Le traitement des données visées à l'alinéa 1 effectué par des organismes publics, à l'exception des établissements publics à caractère économique, n'est admis que s'il est autorisé par une expresse disposition de loi spécifiant les données pouvant être traitées, les opérations pouvant être effectuées et les motifs d'intérêt public importants qui sont poursuivis. A défaut de ladite disposition de loi, et hors des cas prévus par les décrets législatifs de modification et intégration de la présente loi, pris en application de la loi n. 676 du 31 décembre 1996, les organismes publics peuvent demander au *Garante*, dans l'attente d'une disposition normative, d'indiquer les activités, parmi celles qui leur sont conférées par la loi, qui poursuivent d'importantes finalités d'intérêt public et pour lesquelles, conformément à l'alinéa 2, le traitement des données visées à l'alinéa 1 est par conséquent autorisé ...". Voir également dans le même sens la loi portugaise du 26 octobre 1998 qui stipule dans son article 7.2 que "... par disposition légale ou autorisation de la CNPD, le traitement des données visées au paragraphe précédent peut être autorisé lorsque, pour des motifs d'intérêt public important, il est indispensable à l'exercice des fonctions légales ou statutaires de son responsable ou lorsque la personne concernée a donné son consentement exprès au traitement, dans les deux cas avec des garanties de non-discrimination et moyennant les mesures de sécurité prévues à l'article 15.V ...". Voir la loi française et plus spécialement l'article 8 qui stipule que "de même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 (autorisation de la CNIL) ou au II de l'article 26 (autorisation par décret en Conseil d'État après avis motivé et publié de la CNIL). La loi hellénique 2472/1997 de 1997 telle qu'amendée en 2001 prévoit quant à elle dans son article 7 que : "Exceptionally, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, will be permitted by the Authority, when one or more of the following conditions occur : ... e) Processing is carried out by a Public Authority and is necessary for the purposes of aa) national security, bb) criminal or correctional policy and pertains to the detection of offences, criminal convictions or security measures, cc) public health or for the exercise of public control on social welfare services". La Section 20 de la Personal Data Act of Sweden du 29 avril 1998 énonce quant à elle l'exception suivant laquelle : "The Government or the authority appointed by the Government may issue regulations on further exemptions from the prohibition in Section 13 (It is prohibited to process personal data that reveals a) race or ethnic origin, b) political opinions, c) religious or philosophical beliefs, or d) membership of a trade union.) if it is necessary having regard to an important public interest".

ragraphe premier de l'article 53 de toute obligation. Ainsi l'administration publique dans le cadre de la "... sécurité publique ou de la défense nationale, ou pour procéder aux poursuites pénales, ou lorsque ledit traitement s'avère nécessaire à l'exécution de leurs missions conformément aux lois en vigueur" ne peut être limitée ni par le principe de l'interdiction, ni par les conditions des exceptions possibles. Ces personnes publiques ne sont ainsi pas soumises à l'interdiction de l'article 14 et de ce fait se retrouvent autorisées à collecter et traiter les données sensibles librement et sans aucune limite.

Mais la loi va plus loin puisque les personnes publiques du paragraphe premier ne sont même pas soumises à l'obligation prévue par l'article 15⁸⁴ qui stipule que le traitement de ces données est soumis à l'autorisation de l'Instance nationale de protection. Ainsi aucune limitation n'est imposée aux personnes publiques du paragraphe premier et aucune "garantie appropriée" n'est prévue pour protéger les citoyens contre les discriminations possibles.

Mais la loi tunisienne fait bénéficier les personnes publiques du paragraphe premier de l'article 53 d'autres dérogations. En effet, le citoyen au moment de la collecte des données ne peut même pas s'opposer à cette opération.

B. Des fichiers publics "sensibles" sans possible opposition du citoyen

Le citoyen a le droit au moment de la collecte des données à caractère personnel le concernant de s'opposer à l'opération. Ce droit découle du principe que toute personne a droit à la préservation de sa vie privée. L'exercice de ce droit doit être distingué de l'obligation qui pèse sur le maître du fichier d'obtenir le consentement de l'individu au moment de la collecte de ces informations.

Ainsi les législations en droit comparé⁸⁵ stipulent dans leurs dispositions que toute personne dont les données sont traitées peut s'opposer à n'importe quel moment du

⁸⁴ L'article 15 de la loi dispose que : "Le traitement des données à caractère personnel mentionnées par l'article 14 (données sensibles) de la présente loi est soumis à l'autorisation de l'instance Nationale de Protection des données à Caractère Personnel à l'exception des données relatives à la santé. L'instance doit donner sa réponse concernant la demande d'autorisation dans un délai ne dépassant pas trente jours à compter de la date de sa réception. Le défaut de réponse dans ce délai vaut refus. L'instance peut décider d'accepter la demande tout en imposant au responsable du traitement l'obligation de prendre des précautions ou des mesures qu'elle juge nécessaires à la sauvegarde de l'intérêt de la personne concernée".

⁸⁵ Voir la loi fédérale allemande qui dans son article 20.5 dispose que : "... les données à caractère personnel n'ont pas le droit d'être collectées, traitées ou utilisées pour un traitement automatisé ou un traitement dans des fichiers non automatisés si la personne concernée s'y est opposée auprès de l'organisme responsable ...". Voir aussi dans le même sens la loi belge qui dans son article 12§1 dispose que : "... toute personne a en outre le droit de s'opposer ... à ce que des données la concernant fassent l'objet d'un traitement". Voir également la loi française qui en son article 38 énonce le même principe en déclarant que : "... toute personne physique a le droit de s'opposer ... à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ...". Voir la loi luxembour-

processus de traitement des données le concernant à cette opération et y mettre fin. C'est d'ailleurs le sens de l'article 42 de la loi de 2004 en Tunisie⁸⁶ qui donne l'impression d'avoir élargie le cercle des personnes pouvant user de ce droit. En effet, la loi inclue les héritiers ou le tuteur, ce qui nous paraît superflue, au moins pour le tuteur car il agit sur la base du droit de la personne sous tutelle et non sur la base d'un droit qui lui serait propre.

Après avoir énoncé le principe, toutes les législations conditionnent l'opposition. En effet, elle doit revêtir certaines caractéristiques pour être prise en considération. Dans le cas où elle est admise elle entraîne certaines conséquences.

L'article 42 de la loi tunisienne stipule que l'opposition ne peut être admise que pour des "raisons valables, légitimes et sérieuses". La loi allemande évalue chaque situation à part en faisant prédominer "l'intérêt légitime de la personne concernée" sur "l'intérêt de l'organisme responsable". Les lois luxembourgeoise, portugaise et monégasque conditionnent l'acceptation de l'opposition à l'existence de "raisons prépondérantes et légitimes". Enfin toutes les législations rejettent l'opposition possible de la personne concernée quand la collecte des données est réalisée sur la base d'une obligation légale. Il revient à la structure de contrôle dans un premier temps et au juge en dernier ressort de déterminer si les conditions arrêtées par les lois nationales sont réunies dans le cas de l'espèce.

L'opposition de la personne concernée doit mettre fin immédiatement à la collecte ou au traitement des données à caractère personnel. C'est ce qui ressort du paragraphe 3 de l'article 12 qui dispose que "L'opposition suspend immédiatement le traitement". L'article 14 de la directive européenne n°95/46 dispose quand à elle qu'"En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données".

C'était là passé en revue le principe général de l'opposition avec ces conditions et ces exceptions. Qu'en est-il de l'opposition possible contre la collecte et le traitement des données à caractère personnel par les personnes publiques ?

Le deuxième alinéa du paragraphe 54 est clair à ce sujet : la possibilité d'opposition prévu à l'article 42 ne peut être appliquée contre les personnes publiques définies dans le paragraphe premier de l'article 53⁸⁷ -ces personnes mêmes

geoise qui dans son article 30.1 dispose que : "toute personne concernée a le droit : a. de s'opposer à tout moment ... à ce que des données la concernant fassent l'objet d'un traitement ...". Voir enfin la loi monégasque qui stipule en son article 13 que : "toute personne physique ou morale a le droit : 1° de s'opposer ... à ce que des informations la concernant ou relatives à ses membres fassent l'objet d'un traitement ...".

⁸⁶ L'article 42 de la loi tunisienne dispose dans ces premiers termes que : "La personne concernée, ses héritiers ou son tuteur, a le droit de s'opposer à tout moment au traitement des données à caractère personnel le concernant ...".

⁸⁷ L'article 54 de la loi tunisienne dispose dans ces premiers termes que : "... Le traitement réalisé par les personnes mentionnées au premier paragraphe de l'article 53 de la présente loi n'est pas soumis également aux dispositions des articles ... 42 ...".

qui sont habilitées à traiter des données sensibles-. Une dispense qui est confirmée par l'article 58⁸⁸ qui permet aux personnes intéressées de s'opposer au traitement réalisé par les établissements publics définis par l'alinéa deux de l'article 53.

La législation tunisienne se met ainsi en porte à faux avec le consensus international établi sur la question. En effet, les fichiers publics revêtant plus de dangers, pour protéger les individus, les législations permettront aux citoyens mis en confrontation avec les personnes publiques d'utiliser leur droit d'opposition. La seule condition à laquelle les législations soumettent cette opposition est qu'elle soit justifiée par sa légitimité, comme développé *supra*. Pour donner un exemple nous ne citerons que la directive européenne n° 95/45 que les États de l'Union ont intégré dans leurs législations nationales. En effet, celle-ci dispose en son article 14 que "les États membres reconnaissent à la personne concernée le droit : a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment ...". Ainsi les points cités sont la base minimale permise aux États, le prérequis *minima*. Ceux-ci ont toute la latitude de ne pas reconnaître le droit d'opposition mais pas dans le domaine défini par l'article 7 paragraphes e) et f). En retournant à l'article 7 point e de la directive, on trouve qu'il prévoit le traitement quand "il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées". Ce sont là les domaines dont sont investies les personnes publiques et spécialement celles définies par l'article 53 paragraphe premier de la loi tunisienne.

Au vu des dispositions de la loi tunisienne sur la question, on est à même de se poser un certain nombre de questions : comment est-ce que le citoyen va être mis au courant de l'existence du traitement et du fichier pour pouvoir s'y opposer même pour les personnes publiques de l'alinéa deux ? Qui aura à statuer sur les litiges qui surviennent entre l'administration et les citoyens à l'occasion de l'exercice du droit d'opposition ? Les personnes publiques, qui sont emmenés à rendre des prestations aux citoyens, ne vont-elles pas conditionner leur bénéfice à la non opposition à l'acte de collecte des données à caractère personnel ?

A la première question, on renverra le lecteur aux développements *supra* I.A. En effet, les personnes publiques, sont habilitées à créer les fichiers sans informer l'autorité de contrôle ni lui demander l'autorisation pour réaliser cela. Ces deux opérations sont de nature normalement à assurer une certaine publicité des fichiers à côté du contrôle *a priori* sur leur contenu. Ainsi les fichiers publics par définition secrets en Tunisie ne pourront au moment de leur alimentation en données susciter

⁸⁸ L'article 58 de la loi tunisienne dispose que : "La personne concernée, son tuteur, ou ses héritiers peuvent s'opposer au traitement des données à caractère personnel effectué par les personnes mentionnées au deuxième paragraphe de l'article 53 de la présente loi si un tel traitement est contraire aux dispositions de la présente loi qui lui sont applicables".

des oppositions de la part des citoyens qui auront des raisons “valables, légitimes et sérieuses” de s’y opposer.

A la deuxième question, le texte de la loi organique y donne une réponse : en effet, l’article 43 dispose que : “L’instance Nationale de Protection des Données à Caractère Personnel est saisie de tout litige relatif à l’exercice du droit d’opposition”. Mais qu’il nous soit permis de douter, au vu entre autre de sa composition, de l’efficacité de l’action de cette structure quant au contrôle des fichiers publics.

Dans tous les systèmes comparés, la structure de contrôle est un organe bénéficiant d’une indépendance aussi bien administrative que politique lui permettant de jouer un rôle de contrôle mais surtout de conseiller du gouvernement et des pouvoirs publics pour toute action rentrant dans le cadre de la protection des données personnelles. Elle joue aussi un rôle d’information des pouvoirs publics mais aussi de l’opinion publique sur leurs droits et leurs obligations mais aussi les pratiques, les abus constatés dans le domaine ainsi que les avancées technologiques permettant d’améliorer la protection des données personnelles. Dans tous les régimes démocratiques, on a essayé de trouver une position spéciale pour la structure de contrôle afin de préserver son indépendance surtout vis-à-vis du pouvoir exécutif. Car c’est à cette seule condition que la structure de contrôle peut jouer un rôle efficace et impartial.

Le législateur tunisien a condamné l’Instance “dans l’œuf”. Il a commencé par la créer au sein du ministère de la justice et des droits de l’homme. Par la suite sa composition est loin d’être indépendante, elle est même très proche de l’administration⁸⁹. Enfin, elle n’est pas dotée d’assez de pouvoirs lui permettant de protéger l’usager de l’administration contre d’éventuels comportements portant atteinte à ces droits au respect de ces données personnelles. Cette structure est ainsi dotée de “malformations congénitales” qui nous laissent douter même de sa volonté future à défendre les intérêts légitimes des individus contre l’“administration mère”.

A la troisième question, on est en droit de craindre que même les personnes publiques soumises au droit d’opposition des citoyens, pourront vraisemblablement et en pratique “monnayer” les prestations qu’elles rendent aux citoyens en arrachant leurs consentements et leur engagements à ne pas utiliser leurs droits d’opposition en contrepartie de la prestation administrative demandée.

En effet, les législations nationales interdisent cette liaison entre la prestation demandée et le consentement à la collecte et au traitement des données. La loi orga-

⁸⁹ D’après l’article 78 de la loi l’Instance nationale de protection des données personnelles compte 13 membres qui se répartissent comme suit : 6 représentants de départements ministériels, 2 choisis par l’administration et un membre du comité supérieur des droits de l’homme et des libertés fondamentales. Ce qui donne un total de 9 sur 13 membres proches de l’administration publique. Le reste des membres peuvent être considérés comme indépendants puisqu’ils sont 4 magistrats et 2 représentants du pouvoir législatif.

nique tunisienne dispose dans ce sens dans son article 17 qu'“il est, dans tous les cas, strictement interdit de lier la prestation d'un service ou l'octroi d'un avantage à une personne à son acceptation du traitement de ses données personnelles ...”. La disposition est claire ce “chantage” est strictement interdit. Qu'en est-il des personnes publiques ? Rien dans la loi ne s'oppose à appliquer l'article 17 à ces personnes car sa rédaction est générale et la section relative aux fichiers publics ne cite par cette disposition dans les dérogations prévues. L'Instance aura vraisemblablement à statuer sur des affaires évoquant ce genre de problème.

Ainsi les personnes publiques du paragraphe premier de l'article 53 en plus de toutes les “protections” dont ils bénéficient et que nous avons traitées dans la première partie, se retrouvent en ce qui concerne les fichiers sensibles autorisées à les traiter et sans que le citoyen ne puisse s'y opposer et même y accéder.

C. Des fichiers publics “sensibles” sans accès possible du citoyen

Toute personne dont les données sont collectées et traitées doit avoir la possibilité d'y accéder, c'est là un principe repris dans toutes les législations nationales et à commencer par les lignes directrices des Nations Unies et de l'OCDE. Ce principe est considéré comme la “principale garantie” du système de protection des données à caractère personnel⁹⁰ aspirant à la protection de la vie privée des individus.

Ce principe communément admis permet aux citoyens dans un premier temps de savoir si des données les concernant se trouvent dans un système de gestion de fichiers. Dans un deuxième temps l'individu qui a la preuve de l'existence de ces données, peut grâce au droit d'accès en avoir communication et vérifier de cette façon la légalité ainsi que l'intégrité et la mise à jour de ces données personnelles⁹¹.

C'est dans ce sens que la directive européenne 95/45 a considéré que c'était là, la seule manière pour l'individu, de s'assurer de la “licéité” du traitement des données le concernant⁹². Les législations étrangères ont réservé, dans leur grande majorité, une subdivision entière de leur législation à traiter du droit d'accès, de ces condi-

⁹⁰ Voir les lignes directrices de l'OCDE qui disposent dans leur §58 que “le droit des personnes physiques d'avoir accès aux données de caractère personnel et de les contester est, en règle générale, considéré comme étant peut-être la principale garantie de protection de la vie privée. Ce point de vue est partagé par le Groupe d'experts qui, tout en étant conscient du fait que le droit d'accès et de contestation ne saurait être absolu, a décidé de l'exprimer en des termes clairs et assez précis ...”.

⁹¹ Voir les lignes directrices des Nations Unies qui disposent en leur point 4 que “toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexacts, et, lorsqu'elles sont communiquées, d'en connaître les destinataires ...”.

⁹² Voir la directive européenne 95/45 qui dispose à ce propos dans son point 41 que “considérant que toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement ...”.

tions, de ces modalités ainsi que de ces effets et des exceptions au droit de l'exercer.

De ces dispositions on peut faire ressortir les grandes règles concernant ce principe : Le droit d'accès est inaliénable⁹³ et simple à exercer⁹⁴ à des intervalles raisonnables et sans entraîner pour l'individu des frais ou des délais d'attentes excessifs⁹⁵. Il peut être exercé par toute personne qui donne la preuve de son identité⁹⁶ et dans certaines législations est même ouvert aux résidents sans qu'ils soient nécessairement nationaux⁹⁷ ou aux ayants droits⁹⁸.

La loi tunisienne a synthétisé toutes les conditions citées. Elle commence par définir le droit d'accès, ce qu'aucune législation, à notre connaissance, ne prend la peine de faire explicitement⁹⁹. La loi prévoit que ce droit peut être exercé non seulement par l'intéressé, mais aussi par ses héritiers ou son tuteur pour le mineur. Il consiste à avoir la possibilité de consulter les données personnelles qui sont attachées à cette personne. La loi tunisienne considère que ce droit inclus d'autres droits liés repris indépendamment par les législations étrangères : Elle dispose dans le même article que ce droit comprend aussi celui d'avoir communication sous forme intelligible¹⁰⁰ de ces données et éventuellement le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer¹⁰¹.

⁹³ Voir la loi fédérale allemande qui dispose en son article 6 que : "Droits inaliénables de la personne concernée : (1) le droit d'accès de la personne concernée aux données la concernant ... ne peuvent être ni exclus ni limités par un acte juridique ...". Voir la loi helvétique qui dispose en son article 8.6 que "... nul ne peut renoncer par avance au droit d'accès".

⁹⁴ Voir les lignes directrices de l'OCDE qui disposent à ce propos que "59. Le droit d'accès devrait, en règle générale, être simple à exercer. Cela peut signifier notamment qu'il devrait s'inscrire dans le cadre des activités quotidiennes du maître du fichier ou de son représentant et ne nécessiter aucune action juridique ou mesure analogue ...".

⁹⁵ Voir la directive 95/45 de l'Union Européenne qui dispose à ce propos en son article 12 que "les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement : a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs ...".

⁹⁶ Voir la loi française qui dispose en son article 39.I que "toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel ...".

⁹⁷ Voir la loi canadienne qui dispose que "12. (1) Sous réserve des autres dispositions de la présente loi, tout citoyen canadien et tout résident permanent, au sens de la Loi sur l'immigration, a le droit de se faire communiquer sur demande : a) les renseignements personnels le concernant ...".

⁹⁸ Voir la loi luxembourgeoise qui dispose en son article 28.1 que "sur demande à introduire auprès du responsable du traitement, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent obtenir sans frais, à des intervalles raisonnables et sans délais excessifs : (a) l'accès aux données la concernant ...".

⁹⁹ Voir l'article 32 de la loi organique qui dispose qu'"au sens de la présente loi, on entend par droit d'accès, le droit de la personne concernée, de ses héritiers ou de son tuteur de consulter toutes les données à caractère personnel la concernant, ainsi que le droit de les corriger, compléter, rectifier, mettre à jour, modifier, clarifier ou effacer lorsqu'elles s'avèrent inexacts, équivoques, ou que leur traitement est interdit. Le droit d'accès couvre également le droit d'obtenir une copie des données dans une langue claire et conforme au contenu des enregistrements, et sous une forme intelligible lorsqu'elles sont traitées à l'aide de procédés automatisés".

¹⁰⁰ Voir la résolution 95-45 des Nations Unies portant lignes directrices qui dispose en son point 4

Qu'en est-il en Tunisie concernant le droit d'accès aux données détenues par les personnes publiques ? La rédaction de l'article 56 est claire et sans équivoque ne laissant aucune possibilité d'interprétation. En effet, "le droit d'accès aux données à caractère personnel traitées par les personnes mentionnées à l'article 53 ne peut être exercé". Le législateur aurait pu inclure l'article 32 traitant de ce droit dans la liste arrêté dans l'article 54, mais il a voulu, en lui réservant un article spécifique, écarter le droit d'accès dans des termes sans appel. L'effet utile du texte nous confirme ainsi la volonté non équivoque du législateur : le droit d'accès "ne peut être exercé" concernant ces personnes.

Mais tous les fichiers publics ne sont pas, à ce propos, logés à la même enseigne puisque l'alinéa deux de l'article 56 réserve un statut intermédiaire entre les fichiers privés soumis au droit d'accès et les fichiers publics traités par les personnes publiques de l'alinéa premier de l'article 53 : c'est celui des fichiers qui dépendent des personnes publiques définies dans le deuxième alinéa de l'article 53 (établissements publics de santé et établissements publics non administratifs). Dans ce cas là, un droit d'accès "spécial" peut être exercé. En effet, la personne concernée qui se trouve "par hasard" informée de l'existence de données inexactes la concernant a le droit de demander leurs rectifications, mise à jour ou effacement.

que la personne intéressée est en droit "... d'en avoir [des données la concernant] communication sous une forme intelligible, sans délais ou frais excessifs ...". Voir dans le même sens la directive européenne 95/45 qui dispose à ce propos en son article 12 que "les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement :... la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données ...". Voir également la loi belge qui dispose dans son article 10§1 que : "la personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement : ... b) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données ...". Voir la loi française qui dispose en son article 39 que : "I. Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : ... 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ...". Voir l'article 15 de la loi monégasque qui stipule que : "La personne qui a accès aux informations nominatives peut, sous réserve de justifier son identité : ... 2° obtenir communication de ces informations sous une forme écrite, non codée et conforme au contenu des enregistrements en contrepartie du paiement d'une somme forfaitaire, variable selon les catégories de traitement et dont les montants sont fixés par arrêté ministériel pris après avis de la commission de contrôle des informations nominatives ...".

¹⁰¹ Voir la résolution 95-45 des Nations Unies portant lignes directrices qui dispose en son point 4 que la personne concernée a le droit "... d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexacts ..." des données personnelles la concernant. Voir la directive 95/45 de l'Union Européenne qui dispose à ce propos en son article 12 que "Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement : ... b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données ...". Voir la loi monégasque qui dispose en son article 16 que : "La personne intéressée peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou supprimées les informations la concernant lorsqu'elles se sont révélées inexactes, incomplètes, équivoques, périmées ou si leur collecte, leur enregistrement, leur communication ou leur conservation est prohibé".

Comment va-t-on en prendre connaissance !? C'est une question qui reste sans réponse quand on sait que ces fichiers ne sont soumis à aucune procédure de publicité ni de contrôle *minima* de la structure de contrôle. C'est un droit d'accès "virtuel" difficilement applicable en l'état aux citoyens.

Ce que l'on peut ainsi déduire de cette disposition, c'est que les personnes publiques de l'alinéa premier qui sont autorisées à traiter des "données sensibles" ne sont pas soumises au droit d'accès et donc leurs fichiers ne subissent aucune publicité ni demande de communication. Pour bien s'installer dans l'absurde de l'article 56, imaginons un individu qui prend connaissance "par hasard" de données sensibles mais erronées le concernant traitées par ces personnes, il n'a d'après la loi aucun droit d'en demander la rectification ou la mise à jour !!! Ainsi ces fichiers secrets le restent même si on sait qu'ils contiennent des données erronées, inexacts ou illégaux, pouvant servir à des prises de décisions préjudiciables.

Un député a eu à relever au cours des débats parlementaire le problème de l'inexistence du droit d'accès. Il posait ainsi la question de savoir quel était le justificatif de cette interdiction. Le ministre répondit qu'il ne connaissait aucun État où il est permis d'exercer le droit d'accès aux données relatives à la sécurité et la défense¹⁰². Ce que Monsieur le ministre a omis de dire c'est que par contre les législations prévoient des accès indirects qui garantissent aussi bien les droits des individus en préservant les intérêts primordiaux et indiscutables de la nation en matière de sécurité et de défense.

Le droit comparé prévoit généralement deux catégories de droit d'accès. Le premier est dénommé direct car il est exercé par la personne concernée elle-même directement auprès du maître du fichier. Le deuxième est qualifié par contre d'indirect car il ne permet pas à la personne elle-même de l'exercer, mais habilité d'autres personnes prévues dans les législations à le faire à sa place¹⁰³. Cette

¹⁰² السيد محمد المختار الجلاي سيدي الرئيس، بوّدي أن أتساءل حول أسباب عدم إمكانية ممارسة حق النفاذ بالنسبة إلى الأشخاص المنصوص عليهم بالفصل 53 وشكراً.

السيد وزير العدل وحقوق الإنسان لا أعرف دولة يتم فيها النفاذ إلى المعطيات المتعلقة بالأمن العام والدفاع الوطني وذلك هو السبب.
¹⁰³ Voir la loi fédérale allemande qui dispose en son article 6 que : "... (6) Si les informations ne sont pas fournies à la personne concernée, elles peuvent, sur sa demande, être fournies au Délégué fédéral pour la protection des données, sauf si l'administration fédérale suprême compétente constate que dans le cas particulier, cela mettrait en danger la sécurité de l'État fédéral ou d'un Land ...". Voir la loi luxembourgeoise qui dispose en son article 29 concernant les exceptions au droit d'accès que "(1) Le responsable du traitement peut limiter ou différer l'exercice du droit d'accès d'une personne concernée lorsqu'une telle mesure est nécessaire pour sauvegarder : (a) la sûreté de l'État; (b) la défense; (c) la sécurité publique; ... (4) En cas de limitation de l'exercice du droit d'accès de la personne concernée, le droit d'accès est exercé par la Commission nationale qui dispose d'un pouvoir d'investigation en la matière et qui fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi. La Commission nationale peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question ...". Voir la loi portugaise qui dans son article 11 dispose que "... 2. En cas de traitement de données à caractère personnel intéressant la sûreté de l'État, la prévention ou la répression du crime le droit d'accès est exercé par l'intermédiaire de la CNPD ou

deuxième alternative a été prévue pour permettre de contrôler la collecte et le traitement de données qui sont normalement secrets, tels que ceux des renseignements généraux ou ceux comportant un secret militaire ou des données médicales. D'ailleurs les lignes directrices de l'OCDE¹⁰⁴ prévoient que l'accès peut s'effectuer par personne interposée comme un médecin quand il s'agit de données médicales ou des membres de la structure de contrôle pour d'autres types de données.

Concernant ce dernier cas, la meilleure concrétisation est l'accès indirect institué par l'article 41 de la loi de 1978 en France qui prévoit que c'est la commission nationale informatique et libertés qui reçoit ces demandes et celle-ci désigne l'un de ses membres pour exercer au nom de l'intéressé ce droit d'accès¹⁰⁵. On prend conscience de l'importance de ce droit, même indirect, quand on consulte les rapports de la CNIL. A l'étude des rapports annuels d'activité de la structure de contrôle on constate que le nombre des demandes d'accès indirects¹⁰⁶ se révèle ces dix dernières années substantiel et en constante évolution. En effet, la CNIL a reçu depuis sa création 10656 demandes dont 8557 ces dix dernières années qui se répartissent comme suit :

d'une autre autorité indépendante que la loi charge de vérifier le respect de la législation relative à la protection des données de caractère personnel ...".

¹⁰⁴ Voir les lignes directrices de l'OCDE qui disposent à ce propos dans son point 59 que "...parfois, il y aurait peut-être lieu de prévoir un accès intermédiaire aux données ; dans le domaine médical, par exemple, le médecin pourra servir d'intermédiaire. Dans certains pays, les organes de tutelle, tels que les autorités chargées de l'inspection des données, pourront assurer des services analogues ...".

¹⁰⁵ L'article 41 de la loi française de 1978 telle que révisée en juillet 2004 dispose que : "Par dérogation aux articles 39 (droit d'accès) et 40 (droit de rectification), lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.

La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi".

Et l'article 42 de la même loi dispose que : "Les dispositions de l'article 41 (droit d'accès indirect) sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25 (autorisation par la CNIL), 26 (autorisation par décret en Conseil d'État ou arrêté) ou 27 (autorisation par décret en Conseil d'État, arrêté ou décision de l'organe délibérant)".

¹⁰⁶ Commission Nationale Informatique et Liberté, *25^{ème} rapport d'activité 2004*, La documentation française, Paris, 2005, pp. 44-48, *24^{ème} rapport d'activité 2003*, La documentation française, Paris, 2004, pp. 15-16, *23^{ème} rapport d'activité 2002*, La documentation française, Paris, 2003, pp. 12-13

Année	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Nombre	243	320	385	401	671	817	836	1264	1163	2457

D'après le 25^{ème} rapport de la CNIL sur les 2457 demandes d'accès indirects, 89 % ont été réalisés sur les fichiers du ministère de l'Intérieur. Des fichiers énormes y sont mis en place : en France on peut citer à titre d'exemple le "système de traitement des infractions constatées" (STIC) qui est géré par la police nationale pour répertorier les informations issues de toute enquête pénale. Pour avoir une idée de l'importance de ce fichier le 25^{ème} rapport de la CNIL recensait au premier janvier 2004, 5 millions d'individus fichés, 18 millions de victimes pour 26 millions d'infractions traitées. A côté du STIC se trouve son pendant pour la gendarmerie nationale qui se dénomme "système d'information judiciaire" (JUDEX). Il est à noter qu'aussi bien le personnel de la police nationale que celui de la gendarmerie nationale en France peuvent accéder aux deux fichiers. D'aussi grands fichiers engendrent nécessairement des erreurs que relève d'ailleurs la CNIL dans son rapport¹⁰⁷. Des erreurs qui n'auraient pas eu de grandes conséquences si l'utilisation de ces fichiers était restée cantonnée dans le cadre de la finalité de création initiale. Ce que l'on constate, c'est que les personnes publiques et parfois privées, consultent de plus en plus les grands fichiers de sécurité pour éclairer leurs décisions concernant des individus. Cette manière de faire somme toute normale, a le danger d'agrandir le cercle des décisions pouvant être prises sur la base d'informations erronées, incomplètes ou dépassées.

Les demandes de droit d'accès indirects enregistrées en 2004 concernant les fichiers de sécurité intérieure et de défense nationale se répartissent en France comme suit :

MINISTÈRE DE L'INTÉRIEUR		2175
Renseignements généraux (RG)		682
Police judiciaire (PJ)		638
Sécurité publique (SP)		257
Direction de la surveillance du territoire (DST)		50
Système d'information Schengen (SIS)		548
MINISTÈRE DE LA DÉFENSE		282
Gendarmerie nationale (GEND)		231
Direction de la protection de la sécurité de la défense (DPSD)		26
Direction générale de la sécurité extérieure (DGSE)		25

Concernant les données traitées seulement par les services des renseignements généraux, le sort qui a été réservé aux demandes d'accès indirect les concernant est le suivant :

¹⁰⁷ Voir Commission Nationale Informatique et Liberté, *25^{ème} rapport d'activité 2004*, La documentation française, Paris, 2005, pp. 45. Spécialement les 5 cas d'erreurs reportées dans le rapport et qui sont très caractéristiques des conséquences préjudiciables que celles-ci peuvent entraîner pour l'individu "innocent".

Année	2000	2001	2002	2003	2004
Absence de fiches	261	415	776	443	510
Nombre de requérants fichés	104	161	236	243	172
Total des demandes traitées	365	576	1012	686	682
Sort réservé aux demandes					
Dossiers non communicables	18	35	36	26	15
Communication totale	85	126	199	217	157
Communication partielle	1	0	1	0	0

La même procédure est prévue concernant les fichiers de police dans la législation helvétique. Le préposé fédéral à la protection des données traite de cet accès dans la plupart de ces rapports d'activité¹⁰⁸.

Ainsi la loi tunisienne, à l'opposé de la grande majorité des textes comparés, écarte sans appel un autre droit substantiel pour le citoyen. Une autre protection de l'individu tombe face à des personnes publiques dont le pouvoir et la puissance vont jusqu'à leur permettre sans garantie aucune, de traiter les données les plus dangereuses pour la vie privée de l'individu et surtout pour son "avenir social". En effet, des fichiers contenant des données éternelles qui, même dans de petites proportions, peuvent se révéler erronées ou non mises périodiquement à jour, sans parler de celles illégales, entraînent pour les "citoyens" concernés des décisions injustifiées et préjudiciables. Celles-ci peuvent provenir de toute structure questionnant ces bases de données publiques. On s'en aperçoit à l'occasion de refus de recrutement, non seulement au sein de l'administration mais aussi dans les banques et les entreprises privées. On réalise qu'un grain de sable s'est glissé dans les rouages du système à l'occasion de refus répétés d'obtenir des autorisations administratives et parfois même des documents, par exemple de voyage, délivrés par l'administration. Mais les conséquences préjudiciables ne s'arrêtent pas à ce niveau, puisque les personnes publiques du premier alinéa de l'article 53 sont autorisées à collecter et traiter d'autres données "sensibles" sans aucune garantie pour le citoyens : ceux issus des systèmes qui se généralisent dans nos sociétés dénommés de vidéosurveillance.

D. Des fichiers publics de vidéo surveillance sans aucune limite

La vidéosurveillance a été définie comme étant "les systèmes techniques permettant d'assurer la surveillance à distance des bâtiments, des biens et des personnes

¹⁰⁸ On peut lire dans le 7^{ème} rapport d'activité de 1999/2000 du préposé fédéral de protection des données en Suisse à la page 139 ce qui suit : "En vertu de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, toute personne peut nous demander de vérifier si des données la concernant sont traitées conformément au droit par la police fédérale dans le système de traitement des données relatives à la protection de l'État (ISIS). Deux ans après l'entrée en vigueur de cette nouvelle réglementation, une analyse de la mise en application de ce droit d'accès "indirect" peut être tirée en parallèle avec la procédure, en grande partie similaire, du droit d'accès "indirect" prévu dans la loi fédérale sur les Offices centraux de police criminelle de la Confédération (accès aux systèmes DOSIS, ISOK, FAMP et GEWA)".

au moyen de caméras vidéo¹⁰⁹. Les caméras généralement placées dans des lieux publics ou plus précisément ouverts au public permettent suivant leur technologie soit de transmettre des images animées de la scène filmée en permanence, soit de ne le faire qu'au moment où la caméra détecte un mouvement dans son champ de vision. Le sort réservé à ces vidéos est différent suivant la nature de l'installation. Si elle est classique de type analogique, elle enregistre généralement les films obtenus sur une batterie de lecteurs enregistreurs vidéo, si par contre le système est numérique, ils sont généralement stockés sur des disques dur d'ordinateur. Le système de vidéosurveillance est dans ce cas intégré dans une configuration informatique qui facilite non seulement le stockage de l'information mais aussi l'accessibilité et la manipulation des séquences. Ce genre de système peut comprendre un dispositif de détection intelligente et d'alerte automatisé¹¹⁰. Les systèmes numériques de vidéosurveillance peuvent être couplés avec des dispositifs biométriques de reconnaissance faciale. Le même système peut être utilisé par exemple pour reconnaître et enregistrer les caractères composant les plaques minéralogiques des voitures dans un flux de circulation ou à l'accès de tunnels ou de ponts. Les caméras numériques peuvent être manipulées à distance de manière aisée, le système permet de contrôler leurs orientations et de les coupler à des solutions logicielles définissant des zones de masquage dynamique par exemple des fenêtres d'habitations privées. Enfin ces systèmes facilitent la transmission d'images¹¹¹.

Les caméras mises en place pour réaliser de la surveillance sont devenues dans nos sociétés quelque chose de très courant. Les nombreux et récents articles de presse attirent de plus en plus l'attention des citoyens qui ne réalisent généralement pas l'augmentation du nombre de ces dispositifs placés dans les lieux publics. L'information internationale nous fait réaliser le développement de ce phénomène permettant de mettre sous surveillance toute une société. En effet, à l'occasion des derniers attentats terroristes de Londres, on a vu passer à la télévision à plusieurs reprises des images des "coupables" dans le couloir du métro ou dans un autobus obtenues grâce aux systèmes de vidéosurveillance. Ce sont d'ailleurs ces photos diffusées à plusieurs reprises qui ont permis de connaître l'identité réelle des éven-

¹⁰⁹ Forest (D.), *La vidéosurveillance dans les lieux publics et ouverts au public : dispositif et application de la loi du 21 janvier 1995*, Mémoire D.E.S.S. droit du numérique et des nouvelles techniques, Faculté Jean Monnet, Université Paris XI, Septembre 1999, disponible sur le site de juriscom à l'adresse : <http://www.juriscom.net>, p. 2.

¹¹⁰ Le système est alors paramétré pour ne donner l'alerte qu'en cas de survenance d'un événement particulier. Dans les grandes surfaces pour mieux gérer la mise en service des caisses, un système automatique à partir d'images captées par les caméras de surveillance permet la détection des files d'attente et alerte le responsable pour qu'il mette en service d'autres caisses. Le même système permet de donner l'alarme en cas de bouchons dans les artères d'une ville.

¹¹¹ En effet, Internet et les webcams permettent aujourd'hui la transmission sur le réseau international d'images prises en permanence de certains endroits de villes dans le monde. Le même système permet l'installation et la transmission de données en vue de surveiller des endroits bien déterminés à des coûts très réduits.

tuels terroristes et de lancer des avis de recherche les concernant. Mais ces procédés de vidéosurveillance passent la plupart du temps inaperçus : ils sont pourtant placés partout et on les retrouve dans beaucoup d'endroits comme les quais de gare, les halls d'aéroport, les stades, les grandes surfaces mais aussi les petits commerces, les pharmacies, les banques, les parkings, les musées ... La vidéosurveillance s'installe dans notre vie de tous les jours sans que généralement on s'en aperçoive.

Mais il est légitime de se poser la question sur l'importance du phénomène. En Tunisie l'opinion publique ne s'y est pas encore intéressée et de ce fait n'a entraîné ni la publication de statistiques ni suscité un débat public sur la question. Par contre des articles de presse étrangère tracent pour nous un tableau alarmant de la surveillance généralisée de leur société et qui peut, toute proportion gardée, être appliqué à notre société. C'est ainsi que l'on a pu lire sur les pages du Monde que "patrie de George Orwell, inventeur de Big Brother, la Grande-Bretagne est le paradis mondial des caméras de vidéosurveillance". En effet, The Guardian estimait à cette époque (2001) que pas moins de deux millions et demie (2,5) de caméras seraient installées sur le territoire national¹¹². Un autre journaliste rapportait plus récemment sur les mêmes pages que Paris comptait plus de 20000 caméras qui scrutent en permanence les lieux publics et les commerces¹¹³. D'après le même article ces caméras sont reliées à la salle d'information et de commandement de la préfecture de police de la capitale française. Les images arrivent en effet, sur 32 écrans vingt-quatre heures sur vingt-quatre regardées attentivement par une douzaine de policiers. Quatre années plus tard sur les pages du même journal, on était ébahi de savoir qu'un "Londonien est filmé au moins 300 fois par jour"¹¹⁴.

Ces procédés permettent de récolter une masse d'information sur les personnes, leurs déplacements, leurs comportements, leurs activités. Ces données alimentant des fichiers nominatifs entrent dans le cadre de la définition des données à caractère personnel car elles permettent d'identifier les personnes concernées. C'est pour cette raison que de plus en plus, on retrouve dans les législations étrangères de protection de ces informations des dispositions régissant l'utilisation de ce genre de supports¹¹⁵. Dans d'autres pays comme la France on a considéré que le texte sur la

¹¹² Barthélémy (P.), "La Grande-Bretagne, paradis des caméras", *Le Monde*, 22 août 2001.

¹¹³ Bronner (L.) Buffier (D.), "A Paris, 20000 caméras scrutent lieux publics, rues et commerces", *Le Monde*, 5 août 2005.

¹¹⁴ Roche (M.), "un londonien est filmé au moins 300 fois par jour", *Le Monde*, 5 août 2005. Le journaliste y écrit que "Les caméras ont permis l'identification des auteurs des attentats de juillet. Les auteurs des récents attentats de Londres auraient-ils été identifiés sans l'omniprésence des caméras de surveillance urbaine ? Elles fourmillent aujourd'hui dans les stations de métro ainsi qu'aux arrêts d'autobus ...".

¹¹⁵ Voir l'article 3 de la loi luxembourgeoise qui stipule en son article 3 que "... la présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales ...". Voir l'article 4.4 de la loi portugaise qui stipule que : "... la présente loi s'applique à la vidéosurveillance et aux autres formes de captage, traitement

protection des données à caractère personnel régit ce genre de données quand ces systèmes permettent d'alimenter des fichiers contenant des données nominatives¹¹⁶.

La loi tunisienne consacre toute la section IV du chapitre V sur le traitement des catégories particulières de données aux données issues de la vidéo surveillance. Elle commence par déclarer le principe suivant lequel ce genre de procédé doit être autorisé par l'Instance Nationale de Protection des Données à caractère Personnel (article 69). Elle détermine par la suite l'endroit où peuvent être utilisés ces procédés (article 70) : les lieux publics, les endroits en relation avec les transports, les lieux de travail collectif. L'utilisation de la vidéosurveillance est limitée aux besoins de sécurité, de prévention des accidents ou la protection des biens et l'organisation des flux de personnes dans les espaces et dans tous ces cas les enregistrements ne peuvent être sonores (article 71). Les personnes doivent être informées clairement et de manière permanente de l'existence de ces procédés techniques de surveillance (article 72). Ces enregistrements ne peuvent être communiqués que dans des cas circonscrits (article 73) et doivent être détruits à la réalisation de la finalité pour laquelle ils ont été mis en place (article 74). Ce sont là des règles permettant de préserver les droits des individus circulant dans les espaces publics.

La loi tunisienne, comme elle nous a déjà habitué pour d'autres obligations, dans son article 54 soustrait l'administration telle que définie dans l'alinéa premier de l'article 53 à toutes les obligations mentionnées dans la section entière. En effet, on peut y lire que "le traitement réalisé par les personnes mentionnées au premier paragraphe de l'article 53 de la présente loi n'est pas soumis également ... aux dispositions de la quatrième section du cinquième chapitre de la présente loi".

et diffusion de sons et d'images qui permettent d'identifier des personnes dès lors que le responsable du traitement est domicilié ou installé au Portugal ou utilise un fournisseur donnant accès aux réseaux informatiques et télématiques établi sur le territoire portugais ...". Voir le chapitre VII de la loi norvégienne qui comprend les articles 36 à 41. Voir la loi islandaise et plus spécialement ces articles 4 et 24. Voir l'article 6b de la loi fédérale allemande.

¹¹⁶ Voir la délibération n° 94-056 du 21 juin 1994 de la CNIL portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et recevant le public qui déclare dans l'un de ces passages que "les images des personnes doivent être regardées comme des informations nominatives permettant, au moins indirectement, par rapprochement avec d'autres critères, l'identification de ces personnes". Voir Cadoux (L.), *Videosurveillance et protection de la vie privée et des libertés fondamentales*, rapport du 30 novembre 1993 présenté à la CNIL ou elle déclare : "... quelle information, plus qu'une image, mieux que la photo d'une personne, révèle "les origines raciales" de la personne, ou même ses opinions religieuses ?".

Au terme de l'article 10 de la loi française du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, la CNIL n'est compétente pour se prononcer sur les dispositifs de vidéosurveillance que s'ils "sont utilisés pour la constitution d'un fichier nominatif". Mais selon la même loi, c'est au Préfet normalement d'autoriser la mise en place de ce genre de procédé et non à la commission de contrôle.

Encore une fois, l'administration n'est plus tenue de demander l'autorisation de l'Instance pour utiliser ces procédés qu'elle utilise de manière courante aujourd'hui. Ces procédés de surveillance qu'ils soient numériques ou analogiques, liés ou pas à des fichiers nominatifs resteront secrets car aucune publicité ne sera faite pour en informer le public. Aucun droit d'accès ne pourra être exercé sur leur contenu. Si elle le désire, l'administration pourra garder éternellement ces enregistrements, violant un droit de l'homme contemporain, celui du "droit à l'oublié".

CONCLUSION

La lecture des dispositions de la loi organique nous impose de conclure que le système tunisien de protection des données personnelles tunisien est conforme aux standards internationaux sauf en ce qui concerne les fichiers publics. D'après les dispositions de la section première du chapitre cinq de la loi organique, ils continueront à être mis sur pied et gérés dans les antres secrets de "l'administration". Personne ne pourra en connaître l'existence et même ceux qui par pur hasard en ont connaissance ou en présupposent l'existence, ils ne pourront pas en connaître le contenu ni s'opposer à leur traitement et surtout pas en demander leur destruction. Les données à caractère personnel pourront être gardées éternellement, privant tout citoyen du droit à l'oublié revendiqué de plus en plus par les sociétés civiles et transcrit dans les législations nationales de protection des données à caractère personnel.

La loi organique de protection des données personnelles aurait dû s'intituler la loi de protection des données personnelles dans les fichiers privés. Mais la gravité de la situation réside dans le fait que cette immunité à toute épreuve des fichiers publics et surtout ceux gérés par les personnes énumérées dans l'alinéa premier de l'article 53 entraînera pour le citoyen des dommages irréversibles. En effet, les personnes aussi bien publiques que privées se basent de plus aujourd'hui dans leur relation avec le citoyen sur les informations issues de ces fichiers. Ils sont consultés systématiquement à l'occasion de toute opération de recrutement, d'obtention de fonctions, d'autorisation d'activité commerciale ou industrielle. C'est pour ces raisons que toute démarche, auprès aussi bien une personne publique que privée, commence par la déclaration du numéro de la carte d'identité nationale. Un identifiant unique qui permettra de rentrer les données dans les ordinateurs et de ce fait constituera la première information de tout fichier informatisé. La loi tunisienne, contrairement par exemple à celle française n'a pas interdit l'utilisation de cet identifiant unique. Celui-ci a été à l'origine de l'affaire Safari en France qui a donné lieu à la loi de 1978 qui en interdit l'utilisation. Cet identifiant unique pour chaque citoyen permet très simplement la mise en relation des données dispersées dans des systèmes informatiques disparates. L'individu devient ainsi transparent n'ayant plus d'intimité, de vie privée.

Mais alors il est légitime de se poser la question de savoir quel justificatif à cette situation les pouvoirs publics peuvent-ils donner ? La réponse peut être trouvée dans

les débats parlementaires qui se sont déroulés à l'occasion de l'adoption de la loi tunisienne. Un parlementaire s'enquit auprès du Ministre de la justice et des droits de l'Homme du pourquoi de la section dérogatoire concernant les données traitées par les personnes publiques. Celui-ci répondit qu'il avait "... étudié le traitement des données personnelles de la part des autorités publiques, il avait passé en revue vingt-six législations étrangères de pays développés, il a trouvé quelques pays qui avaient par un seul article soustrait l'autorité publique du domaine d'application de la loi en disposant : "cette loi est applicable au traitement des données personnelles, mais pas aux autorités publiques"¹¹⁷. En Tunisie on n'a pas choisi cette option parce que l'on recherche la transparence et la soumission de l'autorité publique au droit. C'est pour cela qu'on l'a soumise à la loi. Mais les spécificités de l'autorité publique justifient la non application de quelques articles de la loi suivant son champ d'intervention"¹¹⁸. Ce qu'a omis de dire le Ministre, c'est que les législations qu'il cite, quand elles écartent l'application de la loi aux personnes publiques, c'est parce que le corpus juridique national a prévu un autre texte spécifique s'appliquant à cette catégorie de personnes. On ne peut donc considérer que les fichiers publics naissent et se développent dans une zone de "non droit", ce à quoi aboutit la loi organique de 2004 et ce qui est contraire à la résolution 45/95 prise dans le cadre de l'Assemblée Générale des Nations Unies. En effet, la résolution détermine les règles applicables en matière de protection des données personnelles pour déclarer en son point 10 que "les présents principes devraient s'appliquer en premier lieu à tous les fichiers informatisés publics et privés"¹¹⁹. Quand l'OCDE a mis au point ses lignes directrices en traitant de leur domaine d'application elle a bien spécifié que "les présentes lignes directrices s'appliquent aux données à caractère personnel, dans les secteurs public et privé ..."¹²⁰. Ainsi, il n'est pas possible de mettre au point une loi de protection qui aboutit à immuniser complètement les fichiers publics de toute obligation ou contrôle.

Le législateur tunisien a apparemment oublié une autre chose très importante. En effet, les pays que le ministre de la justice et des droits de l'homme qualifiait de

¹¹⁷ Nous avons basés notre étude sur 46 textes internationaux ou nationaux (voir la liste en annexe II), dans aucun d'entre eux nous n'avons trouvé ce genre de disposition.

¹¹⁸ السيد البشير التكري، وزير العدل وحقوق الإنسان : وقع التعرض أيضا إلى التصرف في المعطيات الشخصية من طرف السلطة العامة، عند اطلاعنا على القوانين المقارنة واطلعنا على 26 تجربة في الدول المتقدمة هناك بعض الدول استنتجت السلطة العامة من مجال تطبيق القانون وقد جاء فيها فصل : "يطبق هذا القانون على معالجة المعطيات الشخصية ولا يطبق على السلطة العامة"، ونحن في تونس لم نتوجه إلى هذا الخيار لأننا نريد الشفافية ولأن من خيارتنا إخضاع السلطة العامة إلى القانون، فأقررنا أن السلطة العامة خاضعة إلى القانون لكن خصوصياتها تبرر عدم تطبيق بعض الفصول فقط من هذا القانون حسب مجال تدخل هذه السلطة العامة.

Dans le corps du texte c'est nous qui traduisons.

¹¹⁹ Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990. Texte disponible à l'adresse web suivante : <http://daccessdds.un.org/doc/resolution/gen/nr0/567/42/img/nr056742.pdf>

¹²⁰ OCDE, lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980, p. 15. Disponible sur le site de l'OCDE à l'adresse web suivante : <http://www1.oecd.org/publications/e-book/9302012e.pdf>

développés, ont des dispositions très strictes dans leurs lois et qui est synthétisé par la directive européenne quant au transfert transfrontière des données personnelles.

En effet, aucune personne ne peut transférer des données vers un pays tiers que si celui-ci applique des règles de protection équivalentes à celle de son pays¹²¹. La directive parle de protection adéquate ce qui rejoint la notion de protection équivalente issue de la convention 108 de 1981 du Conseil de l'Europe.

C'est ainsi à la commission européenne qu'il revient de prendre la décision de déclarer si un pays a mis en place ou pas une protection adéquate. La Tunisie ne pourra au vu de ce texte bénéficier de cette déclaration. Ceci entraînera des dommages certains à l'économie nationale qui table de plus en plus sur le secteur des services. Les entreprises étrangères ne pourront ainsi plus sous traiter le traitement de leur données en Tunisie. À première vue le législateur tunisien pensant trop à l'efficacité de "l'administration régaliennne" a perdu de vue ce point crucial pour un pays comme le notre.

¹²¹ Voir article 25 de la directive européenne adopté le 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnels, P.E. et C.E., JOCE 23 novembre 1995, n° 1, 281 qui dispose : "1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat. 2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. 3. Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2. 4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause. 5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4. 6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes..."

ANNEXE I.

**LA CONSÉCRATION CONSTITUTIONNELLE
DE LA PROTECTION DES DONNÉES PERSONNELLES**

	Pays	Date	Article
1	Portugal	1976	35
2	Pays-Bas	1989	10
3	Suède	1989	3
4	Croatie	1990	37
5	Slovénie	1991	38
6	Colombie	1991	15
7	Paraguay	1992	135
8	Cap-Vert	1992	42
9	Estonie	1992	42
10	Ex-République Yougoslave de Macédoine	1992	18
11	République Tchèque (charte droits fondam.)	1992	10
12	Slovaquie	1992	19
13	Espagne	1992	18-4
14	Serbie et Monténégro	1992	33
15	Fédération de Russie	1993	24
16	Argentine	1994	43
17	Arménie	1995	20
18	Azerbaïdjan	1995	32
19	Géorgie	1995	41
20	Finlande	1995	10
21	Bosnie Herzégovine	1996	
22	Ukraine	1996	32
23	Pologne	1997	51
24	Albanie	1998	35
25	Hongrie	1998	59
26	Suisse	1999	13
27	Grèce	2002	9A
28	Tunisie	2002	9
29	Timor-Leste	2002	38

ANNEXE II

Textes DE PROTECTION DES DONNÉES PERSONNELLES

		Dénomination	Date	Révision
1	ONU	Résolution Assemblée générale 45/95	14/12/90	
2	OCDE	Lignes directrices	23/09/80	
3	Europe	Convention n° 108	28/01/81	
3*	Europe	Directive 95/46/CE	24/10/95	
4	Allemagne	Loi fédérale de protection des données	01/01/03	
5	Argentine	Personal data protection act	04/10/00	
6	Arménie	Law on personal data	08/10/02	
7	Australie	Privacy act 119	1988	2005
8	Autriche	Federal act concerning the protection of personal data DGS	2000	2001
9	Belgique	Loi relative à la protection des données personnelles	08/12/92	2002
10	Bosnie Herzégovine	Law on protection of personal data	29/07/01	
11	Canada	Loi sur la protection des renseignements personnels et des documents électroniques	13/04/00	2004
12	Chypre	Law 138 (1) The processing of personal data	2001	2003
13	Commonwealth	Privacy model bill		
14	Danemark	Act n° 429 on processing of personal data	31/05/00	
15	Espagne	Organic law 15/1999 on the protection of personal data	13/12/99	
16	Estonie	Personal data protection act	12/02/03	
17	Finlande	Personal data act 523/1999	Mars 1999	24/12/00
18	France	Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés	06/01/78	06/08/04
19	Grèce	Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data	1997	2001
20	Hongrie	Act n° LXIII on protection of PD and disclosure of data of public interest	1992	
21	Honk Kong	Personal data ordinance		
22	Irlande	Data protection act n° 25	13/07/88	2003
23	Islande	Act on Protection of Individuals with regard to the Processing of Personal Data No. 77/2000	2000	
24	Italie	Decreto legislativo n° 196	30/06/03	24/12/03
25	Japon	Personal Information Protection Law	23/05/03	
26	Lettonie	Personal data protection law	23/03/00	24/10/02
27	Liechtenstein	Data protection act	14/03/02	
28	Lituanie	Law n° I-1490 on the public registers (official translation)	13/08/96	
29	Luxembourg	Loi relative à la protection des personnes à l'égard du traitement des don-	02/08/02	

		nées à caractère personnel		
30	Malte	Data protection act	2001	2002
31	Monaco (Principauté)	Loi n° 1.165 réglementant les traitements d'informations nominatives	23/12/93	
32	Norvège	Act n° 31 relating to the processing of personal data	14/04/00	
33	Nouvelle Zélande	Privacy Act	01/07/93	
34	Pays Bas	Personal Data Protection Act	06/07/00	
35	Pologne	Loi sur la protection des données personnelles	29/08/97	2002 2004
36	Portugal	Loi n° 67/98 relative à la protection des données à caractère personnel	26/10/98	
37	République Tchèque	Act on the Protection of Personal Data	04/04/00	
38	Roumanie	Law n° 677/2001 for the protection of persons concerning the processing of personal data and free circulation of such data	22/10/01	
39	Royaume Uni	Data protection act	1998	
40	Slovaquie	Act n° 428 on Personal Data Protection	03/07/02	
41	Slovénie	Personal Data Protection Act	1999	
42	Suède	Personal Data Act	29/04/98	
43	Suisse	Data protection act	19/06/92	
44	Taiwan	Computer processed personnel data protection law	11/08/95	
45	Thaïlande	Official information act	02/09/97	
46	Tunisie	Loi organique n° 2004-63 portant sur la protection des données à caractère personnel	27/07/04	