Droit international

De Terwangne , Cécile; Van Gyseghem, Jean-Marc

Published in:
Vie privée et données à caractère personnel

Publication date:
2013

Document Version
le PDF de l'éditeur

CHAPITRE 2.1.
DROIT INTERNATIONAL

Cécile DE TERWANGNE et Jean-Marc VAN GYSEGHEM

Ce premier chapitre présente les instruments juridiques existant au niveau international, concourant d'une manière ou d'une autre à la protection de la vie privée ou des données à caractère personnel. Par « instruments juridiques internationaux », l'on entend les textes qui dépassent le cadre européen.

Un seul instrument « universel » garantit la protection de la vie privée et de plusieurs aspects y associés ; il s'agit du Pacte international relatif aux droits civils et politiques (point 1). Ainsi qu'on le souligne ci-après, les atteintes au droit à la vie privée protégé par cet instrument peuvent être portées tant devant les juridictions belges que devant l'organe international gardien du Pacte, ce qui présente un intérêt indéniable.

Seul autre instrument juridiquement contraignant présenté sous ce chapitre (point 2), la Convention de Budapest sur la cybercriminalité a été conçue dans le giron du Conseil de l'Europe, mais est ouverte à la signature des pays du monde entier. Associés depuis le début des travaux d'élaboration du texte, les pays tels que les États-Unis, le Japon, le Canada et l'Afrique du Sud assurent le caractère international plutôt que purement européen de la Convention. Cela explique que celle-ci soit mentionnée dans la section consacrée au droit international plutôt que dans celle dédiée au droit européen.

Enfin, deux textes de portée internationale, mais non contraignants, sont présentés, car ils sont incontournables en la matière, ils sont très éclairants et peuvent servir de standard de référence lors d'une négociation mettant en jeu des éléments dépassant les frontières : les Lignes directrices de l'O.C.D.E. (point 3.2.), énonçant depuis plus de trente ans ce qu'on a appelé les « Fair Information Principles » et la Résolution de Madrid (point 4.), texte rédigé en 2009 par un très large ensemble d'autorités nationales de protection des données et contenant une version modernisée, élargie et détaillée des principes de protection des données.

1. Article 17 du Pacte international relatif aux droits civils et politiques (PIDCP)

1.1. Le droit protégé

L'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP) signé à New York le 16 décembre 1966 stipule :

> « 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.
>
> 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Ainsi que relevé dans l'introduction du présent chapitre, cette disposition est la seule disposition juridiquement contraignante, qui protège la vie privée à un niveau universel.

La famille, le domicile et la correspondance sont des facettes « classiques » de la vie privée expressément protégées contre toute immixtion arbitraire ou illégale, à l'instar de ce qui est prévu dans la Convention européenne des droits de l'homme. L'article 17 ajoute à ces aspects la protection de l'honneur et de la réputation. Ces éléments sont intéressants, car ils permettent, dans une certaine mesure, d'exercer un contrôle sur les informations qui se rapportent à soi, à tout le moins sur celles qui véhiculent une image négative qui pourraient conduire à porter atteinte à l'honneur ou à la réputation. C'est d'ailleurs en invoquant une atteinte à cet aspect protégé par l'article 17 que des requérants belges se sont insurgés contre le fait que leurs noms figurent sur une liste noire de l'ONU[1]. Ce cas illustre précisément la question de la maîtrise par un individu des informations le concernant (en l'occurrence les noms et prénoms), question qui est au cœur de l'objet du présent ouvrage.

La Belgique a ratifié le Pacte le 26 avril 1983[2], deux ans après avoir adopté la loi d'approbation de ce traité[3]. La Communauté française avait, quant à elle, adopté un décret d'approbation le 8 juin 1982[4], tandis que la Communauté flamande a fait de même le 25 janvier 1983[5].

---

1. Com. D.H., affaire *Sayadi et Vinck c. Belgique*, 22 octobre 2008. Voy., *infra*, au point 1.2.2., le commentaire plus détaillé de cette affaire.
2. *M.B.*, 6 juillet 1983.
3. Loi du 15 mai 1981 portant approbation des actes internationaux suivants : a) Pacte international relatif aux droits économiques, sociaux et culturels ; b) Pacte international relatif aux droits civils et politiques, faits à New York le 19 décembre 1966, *M.B.*, 6 juillet 1983.
4. Décret de la Communauté française portant assentiment du Pacte international relatif aux droits économiques, sociaux et culturels, fait à New York le 19 décembre 1966, *M.B.*, 15 octobre 1982.
5. Décret de la Communauté flamande portant approbation du Pacte international relatif aux droits économiques, sociaux et culturels, fait à New York le 19 décembre 1966, *M.B.*, 26 février 1983.

La plupart des dispositions du Pacte international des droits civils et politiques, et notamment l'article 17, se sont vu reconnaître un effet direct[1]. L'article 17 peut donc être directement invoqué devant les tribunaux belges, ce qu'il est d'ailleurs abondamment, le plus souvent aux côtés de l'article 8 CEDH.

Il faut savoir que l'on peut également invoquer la violation de cet article devant le Comité des droits de l'homme des Nations unies, à Genève.

1.2. Le recours devant le Comité des droits de l'homme

1.2.1. Le Comité des droits de l'homme

Le Comité des droits de l'homme[2] est l'organe de surveillance responsable du respect du Pacte international relatif aux droits civils et politiques et de ses protocoles facultatifs. Il peut être saisi par les particuliers qui prétendent que leurs droits et libertés ont été violés par un État, si cet État est partie au Pacte international relatif aux droits civils et politiques et au protocole facultatif s'y rapportant.

Or, depuis le 17 août 1994, la Belgique est précisément liée par le Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques[3]. Ainsi, tout particulier relevant de la juridiction de la Belgique qui estime que l'État a violé l'article 17 du Pacte peut soumettre une plainte, appelée, dans ce contexte, « communication individuelle », au Comité des droits de l'homme établi à Genève[4]. Il faut au préalable avoir épuisé les voies de recours internes disponibles, condition que l'on retrouve à l'identique pour la saisine de la Cour européenne des droits de l'homme (Cour eur. D.H.) à Strasbourg.

Le Comité des droits de l'homme est peu familier aux yeux des acteurs juridiques belges. D'après Fr. Krenc même, « d'aucuns éprouvent de vives difficultés à le distinguer du Conseil des droits de l'homme et de la – défunte – Commission des droits de

1. P. Bracquene, « L'effet direct du Pacte international relatif aux droits civils et politiques après l'arrêt de cassation du 17 janvier 1984 », *R.W.*, 1984-1985, pp. 1563 et s. ; Ch. Behrendt et F. Bouhon, *Introduction à la Théorie générale de l'État – Manuel*, coll. de la Faculté de droit de l'Université de Liège, 2e éd., Bruxelles, Larcier, 2010, pp. 488 à 497 ; E. Claes et A. Vandaele, « L'effet direct des traités internationaux. Une analyse en droit positif et en théorie du droit axée sur les droits de l'homme », *R.B.D.I.*, 2001, pp. 411 et s.
2. J. Dhommeaux, « Le Comité des droits de l'homme : 25 ans d'expérience », *in Libertés, justice, tolérance – Mélanges en hommage au doyen Gérard Cohen-Jonathan,* vol. 1, Bruxelles, Bruylant, 2004, p. 664 ; L. Hennebel, *La jurisprudence du Comité des droits de l'homme des Nations unies – Le Pacte international relatif aux droits civils et politiques et son mécanisme de protection individuelle,* Bruxelles, éd. Nemesis-Bruylant, coll. « Droit et justice », n° 77, 2007 ; Fr. Krenc, « La Belgique "condamnée" pour la première fois par le Comité des droits de l'homme sur fond de lutte contre le terrorisme – Cap sur Genève ! », *J.T.*, 2009, pp. 621 et s. ; S. Van Drooghenbroeck, « Bruxelles, Luxembourg, Strasbourg... Genève : les nouveaux itinéraires du principe d'égalité. À propos des constatations Guido Jacobs c. Belgique », *J.T.*, 2005, pp. 221 et 222.
3. *M.B.*, 23 juin 1994. Sur ceci, voy. notamment P. Lambert, « L'approbation du protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques », *J.T.*, 1994, p. 610 ; S. Marcus Helmons, « La Belgique et le protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques », *Rev. trim. dr. h.*, 1996, pp. 74 à 78.
4. En réalité, si deux des trois sessions annuelles du Comité des droits de l'homme se tiennent à Genève, la troisième a lieu à New York.

l'homme. Pour d'autres, c'est son existence même qui est inconnue »[1]. Illustrant le caractère inusité de l'introduction d'un recours auprès de cet organe des Nations unies, S. Van Drooghenbroeck, pour sa part, a qualifié d'« exotique » la démarche d'un particulier belge s'adressant au Comité des droits de l'homme[2]… Cette méconnaissance est due notamment, selon Fr. Krenc, au fait que la doctrine, de même que la presse, « voue une préférence, pour ne pas dire un culte, à la Cour européenne des droits de l'homme et à sa foisonnante jurisprudence »[3].

1.2.2. Les décisions du Comité à l'issue du traitement d'une communication individuelle

Le Comité des droits de l'homme, composé de dix-huit membres indépendants ayant qualité non pas de juges, mais d'experts[4], rend des décisions contenues dans des « constatations ». Ces dernières ne sont pas juridiquement contraignantes pour les États, mais il ne faut pas croire qu'elles sont pour autant sans effet.

On a vu ainsi la Belgique, « condamnée » pour la première fois par le Comité le 22 octobre 2008 à l'occasion de l'affaire *Sayadi et Vinck* pour violation du Pacte international relatif aux droits civils et politiques (notamment de l'article 17), mettre en œuvre tous les moyens diplomatiques nécessaires pour obtempérer à l'injonction du Comité et donner satisfaction aux requérants. Ces derniers, suspectés à tort de collaboration avec les mouvances terroristes, ont de la sorte obtenu la radiation de leur nom de la liste noire établie par le Comité des sanctions du Conseil de sécurité des Nations unies dans le cadre de la lutte contre le terrorisme international[5].

1.2.3. L'intérêt d'un recours devant le Comité des droits de l'homme

La présentation d'une communication individuelle devant le Comité offre une alternative appréciable à l'introduction d'une requête devant la Cour européenne des droits de l'homme, lorsqu'on n'a pas obtenu gain de cause devant une juridiction interne. « Il appartient aux avocats et conseils d'en prendre conscience afin d'utiliser à bon escient l'une ou l'autre des procédures : Strasbourg n'est pas nécessairement la panacée et Genève peut s'avérer utile... »[6].

1. Fr. Krenc, « La Belgique “condamnée” pour la première fois par le Comité des droits de l'homme sur fond de lutte contre le terrorisme – Cap sur Genève ! », *J.T.*, 2009, p. 621.
2. S. Van Drooghenbroeck, « Bruxelles, Luxembourg, Strasbourg... Genève : les nouveaux itinéraires du principe d'égalité. À propos des constatations Guido Jacobs c. Belgique », *op. cit.,* p. 221.
3. *Ibid*.
4. « […] des personnalités de haute moralité possédant une expérience reconnue dans le domaine des droits de l'homme » (art. 28.2 du Pacte.)
5. Sur cette affaire, voy. J.-F. Flauss, « Les “listes noires” de l'ONU devant le Comité des droits de l'homme. Comité des droits de l'homme des Nations unies, *Sayadi et Vinck c. Belgique*, 22 octobre 2008 », *Rev. trim. dr. h.*, 2010, pp. 271 et s. ; Fr. Krenc, *op. cit*., pp. 621 et s.
6. Fr. Sudre et F. Roux, *in* Fr. Sudre (dir.), *La protection des droits de l'homme par le Comité des droits de l'homme des Nations unies – Les communications individuelles*, Actes du colloque organisé à Montpellier, mars 1995, Montpellier, IDEDH-Faculté de droit de l'Université de Montpellier I,, 1995, p. 1.

Il convient de souligner les avantages que la démarche auprès du Comité des droits de l'homme peut présenter, démarche « dont le plaideur astucieux peut tirer d'appréciables bénéfices »[1]. Ainsi, les requérants dans l'affaire *Sayadi et Vinck c. Belgique* ont assurément choisi la bonne instance pour tenter d'obtenir la radiation de leurs noms sur la liste noire de l'ONU : ils risquaient bien de voir leur requête déclarée irrecevable s'ils l'avaient introduite devant la Cour européenne des droits de l'homme, au vu de la jurisprudence de la Cour ; en outre, ils ont obtenu une réponse en deux ans et demi, alors qu'on connaît les délais décourageants pour voir l'aboutissement d'un recours à Strasbourg ; et, enfin, l'impact symbolique et politique de la décision du Comité, organe de l'ONU, a été sans aucun doute plus important que si la décision avait émané d'un organe européen, ce qui a concouru à l'obtention du résultat final (au-delà de la « condamnation » de la Belgique, le geste du Comité des sanctions du Conseil de sécurité) et à la satisfaction des requérants[2].

La radiation des noms des époux Sayadi-Vinck que le Comité des sanctions refusait jusque-là d'opérer, faisant suite à la « constatation » du Comité des droits de l'homme à l'encontre de la Belgique et aux démarches diplomatiques déployées par notre pays en réponse à l'obligation contenue dans la constatation, témoigne d'une véritable reconnaissance de l'autorité du Comité des droits de l'homme en tant que « quasi-juridiction universelle des droits de l'homme »[3].

2. Convention de Budapest sur la cybercriminalité

La Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, a été conçue dans le cadre du Conseil de l'Europe (STE 185), mais elle est ouverte à la signature de tout État dans le monde, ainsi qu'il a été souligné ci-avant dans les remarques introductives de ce chapitre. À titre d'illustration du caractère international de cette Convention, elle a été signée par les États-Unis (de même que ratifiée), le Canada, le Japon et l'Afrique du Sud. La présence de ces États a été souhaitée dès la phase d'élaboration du texte, phase à laquelle ils ont été associés en qualité d'observateurs. En effet, en 2001 et dans les années qui précèdent, ces États représentaient indubitablement les acteurs phares d'Internet hors de l'Europe et étaient, à ce titre, les bienvenus pour atteindre plus efficacement l'objectif fixé, soit l'harmonisation des législations pénales nationales afin de lutter contre la délinquance liée au « cyberespace ».

1. S. Van Drooghenbroeck, *op. cit.*, p. 221.
2. J.-F. Flauss, *op. cit.*, p. 382.
3. Fr. Krenc, *op. cit.*, § 36.

Cette Convention a été signée par la Belgique le jour même de son adoption à Budapest, mais elle n'a été ratifiée que tout dernièrement, le 20 août 2012. La Belgique n'est donc liée par ce texte que depuis le 1er décembre 2012.

Cette Convention est à la croisée entre la recherche d'efficacité de l'action répressive, qui est souhaitable et qu'il faut atteindre ou renforcer, et la protection des droits fondamentaux. Ce sont principalement le droit à la liberté d'expression, le droit à la vie privée et le droit à la protection des données qui sont en jeu. L'équilibre à trouver entre ces deux objectifs, délicat s'il en est, surtout quand il est question d'ajuster les vues d'États de tradition et de culture très différentes, explique que le texte ait été âprement discuté et qu'il n'ait été débloqué qu'au lendemain des attentats du 11 septembre 2001, lorsqu'il est apparu à tous qu'il devenait impérieux de s'accorder sur un instrument qui, sans être parfait[1], aurait le mérite d'exister.

La Convention sur la cybercriminalité comprend des dispositions visant à l'harmonisation des législations des États signataires sur les plans du droit pénal matériel et du droit procédural. Une série de dispositions sont aussi consacrées à l'indispensable coopération qu'il convient de mettre en place ou de renforcer au niveau international[2].

Il n'y a pas lieu de présenter ici de trop amples développements sur le contenu de la Convention, car ces développements sont réservés, pour ce qui intéresse la matière du présent ouvrage, aux chapitres 4 et 12.

On peut toutefois signaler à ce stade que la Convention impose aux États signataires d'ériger en infraction pénale le fait de porter atteinte à la confidentialité des données, via l'accès non autorisé ou l'interception illégale de données, ou le fait de porter atteinte à l'intégrité des données, en les altérant ou en les supprimant, ou à l'intégrité du système informatique[3]. Les États parties doivent aussi sanctionner pénalement les faux informatiques et les fraudes informatiques, pour lutter contre les manipulations de données malintentionnées.

Par ailleurs, les parties doivent permettre à leurs autorités d'imposer la conservation rapide des données, y compris les données relatives au trafic, afin d'en disposer pour des enquêtes[4]. Les « données relatives au trafic » désignent

1. Voy. les critiques soulevées par la Global Internet Liberty Campaign (GILC), qui fédère vingt-deux organisations de défense des libertés individuelles provenant de neuf États européens, des États-Unis, de l'Australie, du Japon et d'Afrique du Sud : à leurs yeux, la Convention dans sa version définitive propose « des mesures disproportionnées, liberticides, attentatoires aux droits fondamentaux et à la souveraineté des États » (disponible sur www.gilc.org).
2. Voy. L. COSTES, « La Convention du Conseil de l'Europe du 8 novembre 2001 : premier traité international contre la "cybercriminalité" », *Lamy Droit de l'informatique et des réseaux*, 2001, n° 142, H, pp. 1 à 7.
3. Par « système informatique », il faut entendre « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ».
4. Article 16, § 1er, de la Convention.

« toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent »[1].

Les États sont donc autorisés à donner une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, et de protéger l'intégrité de ces données « pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation »[2]. Ce blanc-seing pour une conservation de trois mois des données de trafic est le résultat de discussions intenses entre tenants de la protection des droits fondamentaux des individus utilisant les voies d'information et de communication du cyberespace et les autorités répressives. Les fournisseurs d'accès, réticents devant le coût induit par les opérations de conservation et de protection des données, visaient à un raccourcissement de la période de conservation, tout comme les défenseurs des droits de l'homme, même si leur motivation n'était de toute évidence pas la même. La durée de conservation initialement prévue était de un an et a donc été ramenée à nonante jours[3].

Les autorités se voient par ailleurs en droit d'ordonner à une personne présente sur leur territoire de communiquer les données informatiques en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique (art. 18, § 1er, a).

Les autorités peuvent, en outre, imposer à un fournisseur de services offrant des prestations sur leur territoire de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services (art. 18, § 1er, b). La Convention a pris soin de préciser ce qu'il faut entendre par données relatives aux abonnés. Cette expression désigne :

1. Article 1er, d), de la Convention.
2. Article 16, § 2, de la Convention.
3. Il est piquant de noter au passage que les décisions portant sur la durée de conservation des données liées aux communications électroniques admissible au sein d'un État démocratique ont, au fil du temps, évolué. Ainsi, alors que l'on s'accordait sur une durée de nonante jours en 2001, les autorités nationales européennes de protection des données s'indignaient un an plus tard qu'on envisage d'étendre cette durée à douze mois au sein de l'Union européenne : « Les commissaires européens à la protection des données ont constaté avec inquiétude que le troisième pilier de l'Union européenne examine actuellement des propositions qui auraient pour conséquence la conservation systématique et obligatoire des données de trafic relatives à l'usage de tout moyen de télécommunication […] pour une durée d'un an ou plus, afin d'en permettre l'accès aux autorités chargées de vérifier l'application effective de la loi. […] doutes importants quant à la légitimité et la légalité de telles mesures. Lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou toute autre forme d'abus. *La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable* » (Groupe de l'article 29, avis 5/2002 sur la Déclaration des commissaires européens à la protection des données adoptée lors de la Conférence internationale de Cardiff (9-11 septembre 2002) relative à la conservation systématique et obligatoire des données de trafic des télécommunications). Finalement, la directive 2006/24 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications stipule, en son article 6, que les données doivent être conservées pour une durée minimale de six mois et maximale de… deux ans. On est loin des trois mois de la Convention de Budapest.

« toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ».

Il était impératif de préciser cette expression, car, ce faisant, le texte clarifiait le fait qu'il ne vise pas la communication de données de contenu.

Un dispositif d'entraide entre parties[1] permet de faire conserver et d'obtenir la divulgation de données par un autre État signataire de la Convention.

3. Les textes adoptés au niveau de l'Organisation de coopération et de développement économiques (O.C.D.E.)

3.1. Mission

L'Organisation de coopération et de développement économiques (O.C.D.E.) a été établie en 1961 et promeut « les politiques qui amélioreront le bien-être économique et social partout dans le monde »[2].

L'O.C.D.E. décrit ses missions comme suit :

« L'O.C.D.E. offre aux gouvernements un forum où ils peuvent conjuguer leurs efforts, partager leurs expériences et chercher des solutions à des problèmes communs. Nous travaillons avec les gouvernements afin de comprendre quel est le moteur du changement économique, social et environnemental. Nous mesurons la

1. Prévu au chapitre III de la Convention.
2. http://www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html.

productivité et les flux mondiaux d'échanges et d'investissement. Nous analysons et comparons les données afin de prédire les tendances à venir. Nous établissons des normes internationales dans un grand nombre de domaines, de l'agriculture à la fiscalité en passant par la sécurité des produits chimiques »[1].

3.2. Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données

Dans le cadre des missions décrites ci-dessus, l'O.C.D.E. a adopté, en 1980, les « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données » sous forme d'une Recommandation. Ces lignes directrices sont en cours de révision. L'achèvement des travaux est prévu en avril 2013.

Ce document, assez précurseur dès lors qu'il est antérieur à toute autre réglementation internationale en la matière, repose sur les trois piliers de l'O.C.D.E., à savoir : « la démocratie pluraliste, le respect des droits de la personne humaine et l'économie de marché ouverte »[2]. Le texte se veut donc une alchimie entre droits humains fondamentaux et économie de marché ouverte.

En guise de préface, le document énonce :

> « Les Lignes directrices sur la vie privée représentent un consensus international sur des orientations générales concernant le recueil et la gestion d'informations de caractère personnel. Les principes énoncés dans ces Lignes directrices se caractérisent par leur clarté et leur souplesse d'application et par leur formulation, qui est suffisamment générale pour leur permettre de *s'adapter au changement technologique*. Les principes couvrent l'ensemble des supports pour le traitement informatisé de *données relatives aux personnes* (depuis les ordinateurs locaux jusqu'aux réseaux aux complexes ramifications nationales et internationales), *tous les types de traitement* de données de caractère personnel (depuis l'administration du personnel jusqu'à la compilation de profils de consommateurs) et *toutes les catégories de données* (depuis les données de trafic jusqu'aux données sur les contenus, et des plus banales aux plus sensibles). Les principes sont applicables aux échelons tant national qu'international[3]. Au fil des ans, ils ont été repris dans un grand nombre d'instruments nationaux, s'appuyant aussi bien sur la réglementation que sur l'autorégulation, et ils sont toujours largement utilisés dans les secteurs tant public que privé »[4].

1. http://www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html.
2. Annexe 1, p. 7, http://www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html.
3. À noter que cette préface a été actualisée au fil des ans, ce qui justifie la référence à des instruments juridiques qui lui sont postérieurs.
4. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html, pp. 7 et 8 ; nous soulignons.

L'objectif économique qui sous-tend les Lignes directrices est, au demeurant, logique dès lors que l'O.C.D.E. a pour mission « de promouvoir les politiques qui amélioreront le bien-être économique et social partout dans le monde »[1].

Il est intéressant de relever que ces Lignes directrices[2] contiennent ce que l'on appelle les « Fair Information Principles » et posent donc les principes fondateurs de la protection des données à caractère personnel[3]. Ces principes de base de la protection des données sont presque identiques à ceux contenus dans la Convention 108 et la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, « directive 95/46 ») qui sera analysée plus loin, textes qui lui sont postérieurs. Cependant, à la différence de ces derniers, ils ne sont pas juridiquement contraignants.

L'O.C.D.E. définit trois termes, qui sont :

– le « maître de fichier » : il s'agit d'une personne physique ou morale qui est habilitée à décider du choix et de l'utilisation des données à caractère personnel ;
– les « données à caractère personnel » : il s'agit de « toute information relative à une personne physique identifiée ou identifiable » qui est la personne concernée ;
– le « flux transfrontière de données à caractère personnel » : il s'agit de la circulation de données à caractère personnel entre pays.

3.2.1. Principes

Champ d'application

Le texte s'applique tant au domaine privé qu'au domaine public sans distinction tel que cela est repris dans son champ d'application énoncé au paragraphe 2 des Lignes directrices :

> « Les présentes lignes directrices s'appliquent aux données de caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles. »

Si l'O.C.D.E. a mis en place un texte ayant un vaste champ d'application (visant tant le domaine privé que le domaine public sans distinction), elle a prévu des possibilités de dérogations au nom d'intérêts publics ou privés prépondérants.

1. www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html.
2. http://www.oecd.org/document/18/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html.
3. Il aurait sans doute été moins ambigu de parler de lignes directrices régissant la protection des données à caractère personnel. En effet, la protection des données à caractère personnel touche plusieurs droits fondamentaux, et pas uniquement la vie privée.

Il est également utile de relever que le texte se veut technologiquement neutre, ce qui signifie qu'il ne veut pas viser une technologie particulière au détriment d'une autre, compte tenu de l'évolution rapide desdites technologies[1].

Transparence

Le traitement de données à caractère personnel doit être effectué en toute transparence (finalités, type de données, etc.) de manière telle que la personne concernée en soit informée et qu'elle puisse exercer ses droits tels que les droits d'accès, de rectification et de recours.

Finalités

L'O.C.D.E. affirme le caractère fondamental de la détermination des finalités pour lesquelles les données sont traitées au moment de la collecte (au plus tard) et que le traitement ne pourra avoir lieu que dans le cadre de ces finalités à l'exclusion de toute autre, sauf exception de compatibilité. Cette exception consiste en la possibilité de poursuivre une autre finalité qui ne soit pas incompatible avec la ou les premières. Pour savoir si une finalité est compatible ou pas, on utilisera – entre autres – le critère de la conscience par la personne concernée qu'une telle finalité pouvait être poursuivie.

Qualité des données

Par ailleurs, seules les données nécessaires à la finalité du traitement pourront être collectées et traitées. Il s'agit d'un principe récurrent et figurant également dans de nombreux autres textes relatifs à la protection des données à caractère personnel. Cela implique également le concept de pertinence qui est directement lié à la finalité du traitement.

De plus, les données traitées doivent être exactes, ce qui implique qu'elles doivent être complètes et mises à jour.

Les données ne peuvent pas, par ailleurs, être conservées au-delà du temps nécessaire pour atteindre la finalité.

Il est utile de préciser que les Lignes directrices n'opèrent pas de différences entre les types de données – sensibles ou pas –, même si elles laissent une marge d'appréciation pour les pays membres pour appliquer les principes de la Recommandation à certains traitements, mais pas à d'autres. Cela ne constitue cependant pas une différenciation entre types de données dans un même instrument.

1. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html, pp. 7 et 8.

Cela est clairement expliqué dans l'exposé des motifs :

> « On pourrait faire valoir qu'il est à la fois possible et souhaitable d'énumérer les types ou catégories de données qui sont en soi sensibles et dont la collecte devrait être limitée, voire interdite. Il existe, dans la législation européenne, des précédents à cet effet (race, convictions religieuses, casier judiciaire par exemple). En revanche, on peut soutenir qu'aucune donnée n'est en elle-même de nature privée ou sensible, mais peut le devenir selon son contexte et l'utilisation qui en est faite. Cette opinion se reflète notamment dans la législation des États-Unis relative à la protection de la vie privée.
>
> Le Groupe d'experts a examiné un certain nombre de critères de sensibilité, tels que le risque de discrimination, mais a estimé qu'il n'était pas possible de définir un ensemble de données qui soient universellement tenues pour sensibles. En conséquence, le paragraphe 7 contient simplement une déclaration générale, selon laquelle des limites devraient être assignées à la collecte des données de caractère personnel »[1].

Sécurité/confidentialité

Les données à caractère personnel doivent faire l'objet d'une protection contre toute détérioration, destruction ou tout accès/utilisation non autorisé. La sécurité telle que prévue dans le texte est tant technique qu'organisationnelle. Cela implique tant les mesures techniques à prendre qu'une dimension de formation du personnel traitant les données et de hiérarchisation des accès aux données[2].

Sanction

Les Lignes directrices ne prévoient pas de sanction comme telle, mais prévoient un principe de responsabilité dans le chef du maître de fichier en son paragraphe 14 :

> « Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus. »

3.3. Déclaration sur les flux transfrontières de données

Constatant que les technologies se développent extrêmement vite et que la conséquence en est une augmentation des flux de données à caractère personnel, et plus particulièrement au niveau de ses États membres, l'O.C.D.E. a adopté sa « Déclaration sur les flux transfrontières de données » le 11 avril 1985.

1. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html, p. 44, §§ 50 et 51.
2. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html, p. 47, § 56.

À l'instar des Lignes directrices vues ci-dessus, l'objectif est économique et se concrétise par une déclaration d'intentions de la part des États membres dès lors que les flux de données jouent un rôle important dans les économies nationales et qu'il faut « porter attention aux questions politiques »[1] qui y sont liées.

3.4. Déclaration relative à la protection de la vie privée sur les réseaux

En 1998, l'O.C.D.E. a adopté une « Déclaration relative à la protection de la vie privée sur les réseaux »[2] par laquelle les États membres réaffirment « leur engagement à l'égard de la protection de la vie privée sur les réseaux mondiaux, afin d'assurer le respect de droits importants, de construire la confiance dans les réseaux mondiaux et d'empêcher des restrictions inutiles aux flux transfrontières de données de caractère personnel » et qu'« ils s'attacheront à établir des passerelles entre les différentes approches adoptées par les pays membres en vue de garantir la protection de la vie privée sur les réseaux mondiaux sur la base des Lignes directrices de l'O.C.D.E. ».

Il s'agit, à nouveau, d'une déclaration d'intentions de la part des États membres.

3.5. Recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée

En 2007, l'O.C.D.E. a adopté une nouvelle « Recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée »[3] mettant en valeur la coopération transfrontière, partant de la constatation que

> « [l]a mondialisation, l'émergence de modèles économiques de “suivi du soleil”, l'essor de l'Internet et l'effondrement des coûts des télécommunications augmentent considérablement le volume des informations de caractère personnel qui franchissent les frontières. Cet accroissement de la circulation transfrontière de l'information a des retombées positives tant pour les organisations que pour les personnes en abaissant les coûts, en induisant des gains d'efficience et en améliorant le service au client. Dans le même temps, ces flux d'informations de caractère personnel accentuent les préoccupations pour la vie privée, en soulevant de nouveaux problèmes de protection des informations de caractère personnel des individus »[4].

1. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html, p. 59.
2. *Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*, www.oecd.org/document/18/0,3746,fr_2649_34255_1815225_1_1_1_1,00.html.
3. www.oecd.org/dataoecd/12/48/38876531.pdf.
4. www.oecd.org/dataoecd/12/48/38876531.pdf, p. 4.

Face à ce constat et au risque que « les personnes perdent leur capacité d'exercer leurs droits à la vie privée, ou de se protéger contre l'utilisation ou la divulgation illicite de cette information »[1], cette Recommandation promeut la coopération entre pays en vue d'une application effective des législations relatives aux données à caractère personnel.

Ce document a également prévu l'établissement d'une autorité de contrôle par les pays membres.

3.6. Conclusion

Si ces divers textes ne sont pas contraignants en tant que tels, ils peuvent servir de base de négociations entre parties et principalement entre parties dont l'une n'est pas soumise au droit européen.

4. La Résolution de Madrid sur des normes internationales de vie privée

4.1. Objectifs

La Résolution de Madrid[2] de 2009 – à ne pas confondre avec la Déclaration de Madrid qui a été adoptée au même moment en vue d'un processus de pétition – est issue d'un travail conjoint des autorités de protection des données de cinquante pays – soit au-delà des frontières de l'Union européenne – sous la houlette de l'Agence espagnole de la protection des données. Elle vise à offrir un modèle reprenant les standards universels de la protection des données, ainsi qu'à réaliser l'intégration des valeurs et principes de protection des données garantis sur les cinq continents.

La Résolution de Madrid est donc un instrument non contraignant qui peut servir à l'adoption ou la modification de régimes de protection des données à caractère personnel par les États signataires sans qu'ils y soient obligés.

L'objectif premier de ce texte est de faciliter les flux transfrontières, point qui ne soulève pas les mêmes questions de protection des données à caractère personnel dans les pays. Comment doit procéder un responsable de traitement qui souhaite

1. www.oecd.org/dataoecd/12/48/38876531.pdf, p. 4.
2. *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data*, www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

transférer des données à caractère personnel vers un partenaire situé à l'étranger ? Comment peut-il s'assurer que le régime de protection en vigueur dans ce pays tiers assure une bonne protection ?

Ce texte souhaite donc faciliter ces transferts en proposant des règles « universelles » de protection des données à caractère personnel.

4.2. Champ d'application

La Résolution fixe, sous réserve de dérogations possibles, son champ d'application à l'article 3 qui est assez proche de celui de la Convention 108 du Conseil de l'Europe qui sera analysée plus loin. Cette disposition est libellée comme suit :

> « Ce document vise dans son application tout traitement de données personnelles, automatisé en tout ou en partie, ou sinon de manière organisée, et mis en œuvre par les secteurs public ou privé. »

4.3. Principes

Nous retrouvons dans cette Résolution nombre de principes déjà relevés par ailleurs dans les Lignes directrices de l'O.C.D.E. (*cf. supra*).

Transparence

Le principe de transparence est traité de façon détaillée à l'article 10 qui prescrit, entre autres, que chaque responsable de traitement doit avoir une politique transparente en matière de traitement de données à caractère personnel. Cette transparence est également le fil conducteur des droits de la personne concernée, tels les droits d'information et d'accès.

Finalité

À la différence de ce qui a été explicité concernant les Lignes directrices de l'O.C.D.E., il est notable de relever que la Résolution de Madrid inclut dans le concept de finalité celui de légitimité[1], dans la ligne de ce qui figure dans la directive européenne 95/46 qui sera évoquée dans un point ultérieur.

1. Article 7.1 de la Résolution : « Le traitement de données personnelles devrait être limité à la réalisation des finalités spécifiques, explicites *et légitimes* de la personne responsable. » (Nous soulignons.)

Par ailleurs, la légitimité du traitement est plus amplement traitée aux articles 12 et 13 de la Résolution qui prévoient les hypothèses dans lesquelles on peut traiter des données personnelles (art. 12) et le régime à réserver aux données sensibles (art. 13 – voy. *infra*).

Qualité des données

La Résolution de Madrid traite de la qualité des données en général[1], à l'instar de l'O.C.D.E., ainsi que de la période durant laquelle elles peuvent être conservées[2].

Cependant, et ce, contrairement à l'O.C.D.E., une distinction entre données « normales » et données « sensibles » est opérée[3], passant de l'autorisation de principe de traiter les données vers une protection accrue des données, celle-ci correspondant souvent à la mise en place d'un régime général d'interdiction. En effet, l'article 12.1.b prévoit que le traitement est légitime « [l]orsque l'intérêt légitime de la personne responsable justifie le traitement, dès lors que les intérêts légitimes, droits et libertés de la personne concernée ne prévalent pas ». Cela signifie en clair que le responsable de traitement pourra traiter les données à condition que des droits fondamentaux dont peut se prévaloir la personne concernée ne s'y opposent pas. Par contre, en présence de données sensibles, l'article 13 prescrit de prévoir des garanties complémentaires. Dans la pratique, l'on constate qu'à titre de garanties complémentaires, les États optent pour un principe général d'interdiction de traitement de telles données moyennant des exceptions limitées à l'interdiction, sans aucune disposition équivalant à celle de l'article 12.1.b. vu ci-dessus. Cette manière de procéder est celle reprise dans la directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données qui sera analysée plus loin. C'est en cela que l'on considère classiquement que les données normales se trouvent dans un régime d'autorisation, tandis que les données sensibles sont protégées par une règle d'interdiction avec des exceptions devant être analysées de manière stricte.

Proportionnalité/nécessité

Le principe de proportionnalité/nécessité est repris clairement aux articles 9 et 12 – mais également implicitement à l'article 8 – de manière répétitive compte tenu de son caractère fondamental, dès lors qu'il intervient tant au niveau des données qu'au niveau du traitement lui-même.

1. Article 9.1. : « La personne responsable devrait en tout temps s'assurer que les données personnelles sont exactes, suffisantes et tenues à jour de telle sorte qu'elles remplissent les finalités pour lesquelles elles sont traitées. »
2. Article 9.2 de la Résolution : « La personne responsable devra limiter la durée de conservation des données personnelles traitées au minimum nécessaire.
   Ainsi, lorsque les données personnelles ne sont plus nécessaires pour atteindre les finalités qui ont légitimé leur traitement, elles doivent être effacées ou rendues anonymes. »
3. Voy. articles 12 et 13 de la Résolution.

Sécurité

À l'instar de l'O.C.D.E., la Résolution de Madrid prescrit une obligation de sécurité tant au niveau technique qu'au niveau organisationnel[1].

L'article 21 prévoit également un devoir de confidentialité ainsi qu'une obligation de notification à la personne concernée de toute faille de sécurité susceptible d'affecter de manière significative ses droits pécuniaires ou non pécuniaires, ainsi que des mesures prises pour la résolution de telles failles[2]. Cette obligation de notifier tout *security breach* est considérée comme essentielle pour permettre à la personne concernée d'exercer son droit à l'autodétermination et de contrôler le sort de ses données[3].

Mesures proactives

La Résolution de Madrid contient un élément tout à fait nouveau au regard du contenu des autres textes internationaux : il s'agit de l'invitation à encourager la mise en œuvre de mesures proactives visant à assurer une meilleure conformité aux règles de protection des données[4]. À titre d'illustration de telles mesures, le texte évoque les mesures visant à prévenir et à détecter les failles de sécurité, la désignation d'un correspondant à la protection des données, la réalisation d'études d'impact pour la vie privée…

Droits de la personne concernée

Des droits sont reconnus à la personne concernée dans la ligne de ce qui existe par ailleurs, mais le catalogue est étoffé : droit d'accès, droit de rectification des données et droit d'opposition.

Le droit d'accès est étendu jusqu'à englober l'accès aux informations concernant l'origine des données[5].

Au droit de rectification des données incomplètes, inexactes, non nécessaires ou excessives, la Résolution de Madrid joint le droit d'obtenir l'effacement de telles données. Ce double droit s'accompagne d'un « droit de suite » consistant dans le fait que le responsable du traitement doit aviser les tiers auxquels les données ont été divulguées – dans la mesure où il les connaît – des modifications intervenues sur les données[6].

1. Voy. articles 20 et 21 de la Résolution. *Cf.* la partie sur l'O.C.D.E.
2. Article 20.2 de la Résolution.
3. Cette obligation est reprise, p. ex., dans la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).
4. Article 22.
5. Article 16.1 : « La personne concernée a le droit d'obtenir, à sa demande, auprès de la personne responsable des informations sur les données personnelles spécifiques sujettes à traitement, ainsi que sur l'origine desdites données, les finalités du traitement et les destinataires ou catégories de destinataires auxquels lesdites données sont ou seront divulguées. »
6. Article 17.

Un droit d'opposition figure également au tableau des droits reconnus[1]. Il présente deux facettes. La première correspond au droit d'opposition consacré dans la directive européenne 95/46 et permet à la personne concernée de s'opposer au traitement de ses données personnelles au nom d'un motif légitime tenant à sa situation personnelle spécifique. La deuxième facette consacre le droit de s'opposer aux décisions qui produisent des effets juridiques basées exclusivement sur un traitement automatisé de données à caractère personnel. Cette facette est originale car elle fait entrer dans les standards internationaux ce qui est présenté dans la directive 95/46 comme un droit autonome (le droit de ne pas être soumis à une décision exclusivement automatisée), mais qui est donc présenté ici sous la forme d'une manifestation particulière du droit d'opposition. Il est clair que cette approche est bien plus fragile qu'une consécration sous forme de droit. Aborder cela par le biais du droit d'opposition n'offre pas la proclamation symbolique que l'homme ne doit pas être soumis à la décision d'une machine.

Accountability

Une autre nouveauté de la Résolution de Madrid réside dans l'introduction, à l'article 11, du concept d'« accountability »[2] qui impose aux responsables « qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent »[3]. Cela signifie que le responsable a la charge de s'assurer que les dispositions de protection des données à caractère personnel sont respectées et de prendre les mesures nécessaires pour y parvenir. Il doit, en outre, mettre en place les mécanismes internes permettant de démontrer aux personnes concernées ou aux autorités de contrôle qu'il s'est conformé aux règles de protection.

Transferts internationaux

Il n'est guère étonnant que la Résolution de Madrid traite des transferts internationaux de données à l'article 15 dès lors que c'est l'un des objectifs du texte. Le principe consiste en ce que les transferts sont autorisés lorsque l'État destinataire des données offre, au minimum, le niveau de protection prévu par la Résolution. Si tel n'est pas le cas, le transfert peut être effectué si des mesures de type contractuel ou autres offrent ce niveau de protection. Les transferts de données vers des pays n'offrant pas le niveau de protection attendu sont aussi permis lorsque cela est nécessaire et dans l'intérêt de la personne concernée dans le cadre d'une relation contractuelle, ou pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne, ou lorsque cela est requis par la loi sur la base d'un intérêt public important.

1. Article 18, § 3.
2. Dès lors que ce terme est très difficilement traduisible en français, nous le laisserons en anglais dans le texte.
3. Groupe de travail de l'article 29, avis n° 3/2010 sur le principe de la responsabilité, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf.

Sanction

Si le texte ne parle pas de sanction, il aborde la question de la responsabilité à l'instar de l'O.C.D.E., en son article 24 :

« 1. La personne responsable sera responsable des dommages et intérêts pécuniaires et non pécuniaires causés à la personne concernée à raison du traitement de données personnelles en violation des lois applicables sur la protection de la vie privée en relation avec le traitement de données personnelles, à moins que la personne responsable puisse démontrer que le dommage ne lui est pas imputable. Cette responsabilité est sans préjudice des actions que pourrait mener la personne responsable contre les sous-traitants impliqués à l'une quelconque des étapes du traitement.

2. Les États promeuvent des mesures adéquates afin de faciliter l'accès des personnes concernées aux voies de recours judiciaires et administratives qui leur permettent d'obtenir réparation d'un dommage tel que mentionné dans le paragraphe précédent.

3. La responsabilité susmentionnée existera sans préjudice des sanctions pénales, civiles et administratives applicables en cas de violation du droit national relatif à la protection de la vie privée concernant le traitement des données personnelles.

4. La mise en place de mesures proactives telles que décrites à l'article 22 de ce document devra être considérée comme un élément déterminant la responsabilité et les pénalités prévues par le présent article. »

4.4. Conclusion

Si ce texte n'est pas contraignant en tant que tel, il peut servir de base de négociations entre parties et principalement entre parties ou même à l'égard de pouvoirs publics, le cas échéant.

5. Tableau récapitulatif

	O.C.D.E.	Résolution de Madrid
Définitions	Paragraphe 1er	Article 2
Détermination des finalités	Paragraphe 9	Article 7
Légitimités	Non explicite	Article 7 Article 12 Article 13
Nécessité/proportionnalité	Paragraphe 7 Paragraphe 10	Article 8 Article 12
Qualité des données	Paragraphe 8	Article 9
Données particulières	Refusé	Article 13
Sécurité	Paragraphe 11	Article 20
Confidentialité		Article 21
Transparence	Paragraphe 12 Paragraphe 7 (application)	Article 10 Article 16 (application)
Droits de la personne concernée	Paragraphe 13	Article 16 Article 17 Article 18
Sanction	Paragraphe 14	Article 25
Autorité de contrôle	Recommandation 2007	Article 23
Flux transfrontières	Recommandation 2007	Article 15