

Protection des données personnelles dans la loi Algérienne*

D. ABDELLI Naima

Chercheur en droit

Email : naimaabdelli@hotmail.com

Résumé

La communication des données en-dehors du champ d'application d'une loi nationale de protection des données risque d'affaiblir considérablement la protection des données. Cet article limite en particulier les droits découlant du respect de la vie privée si le destinataire n'est pas lui-même soumis à des normes de protection des données suffisantes découlant notamment des standards de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel. Les personnes concernées et les autorités de contrôle se voient ainsi démunies du fait de la perte de maîtrise sur les données qui échappent lors de leur transfert aux dispositions nationales de protection des données. Il est dès lors important que les flux transfrontières de données à caractère personnel soient encadrés et que les autorités de protection des données soient en mesure de veiller à ce que les principes de la protection des données soient pris en compte lors de transferts pour garantir le respect de la vie privée des individus et des droits qui en découlent.

Mots clés :

Données personnel, flux transfrontières, protection des données.

Protection of personal data in Algerian law

ABSTRACT

Communication of data outside the scope of a national data protection law risks considerably weakening data protection. This article limits in particular the

* Date de la réception de l'article 18/03/2020, date de révision 13/04/2020, date d'acceptation à la publication 29/05/2020.

rights arising from respect for privacy if the recipient is not himself subject to sufficient data protection standards deriving in particular from the standards of the Council of Europe Convention for the protection of persons with regard to automatic processing of personal data and its additional protocol. The data subjects and the supervisory authorities are thus deprived due to the loss of control over the data which escapes during their transfer to the national data protection provisions. It is therefore important that cross-border flows of personal data are supervised and that data protection authorities are able to ensure that the principles of data protection are taken into account during transfers to ensure compliance the privacy of individuals and the rights that flow from it.

Keywords:

Personal data, cross-border flows, Data protection.

حماية المعطيات الشخصية في القانون الجزائري**ملخص**

إن عملية إيصال للمعطيات ذات الطابع الشخصي خارج نطاق القانون، دون تكريس أي حماية سواء وطنية أو دولية سيؤدي إلى إضعاف هذه الأخيرة، يحدد هذا المقال على وجه الخصوص الحقوق الناشئة عن مدى احترام خصوصية الأشخاص إذا كان المستلم لهذه الأخيرة لا يخضع هو نفسه لمعايير حماية المعطيات ذات الطابع الشخصي بما فيه الكفاية و بشكل خاص تلك الناشئة عن معايير اتفاقية الاتحاد أوروبي لحماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية وبروتوكولها الإضافي. في ظل غياب القوانين والأحكام الخاصة بحماية البيانات الوطنية، يمكن حرمان الأشخاص والسلطات الإشرافية المعنيين بالبيانات بسبب فقدان السيطرة عليها والتي تهرب أثناء نقلها. لذا من المهم مراقبة تدفق البيانات الشخصية عبر الحدود وأن تكون سلطات حماية البيانات قادرة على ضمان أخذ مبادئ حماية البيانات في الاعتبار أثناء عمليات النقل لضمان الامتثال للخصوصية الأفراد والحقوق التي تتدفق منها.

الكلمات المفتاحية:

المعطيات الشخصية، التدفقات عبر الحدود، حماية المعطيات الشخصية.

Introduction

Partons du constat selon lequel les technologies de l'information et de la communication (TIC) se développent non seulement à un rythme infiniment plus rapide que les réformes juridiques, mais qu'elles évoluent également dans un environnement marquée par un «vide juridique», car les lois existantes ne sont plus pertinentes. Cela nous conduit à une situation paradoxale dans la mesure où les règles afférentes au fonctionnement des TIC sont définies et imposées, non pas par l'Etat, mais par des acteurs nationaux et étrangers dominant le secteur. L'article 4 du Règlement général sur la protection des données définit la donnée à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Cette définition est légèrement plus approfondie que celle qui figurait à l'article 2 de la directive 95/46/CE, laquelle précisait que la personne devenait identifiable «*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* ».

Le législateur Algérien a défini les données personnelles comme étant : « *toute information, quel qu'en soit son support, concernant une personne identifiée ou identifiable, ci-dessous dénommée « personne concernée* », d'une manière directe ou indirecte, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale ».

Collecter et traiter des données personnelles implique avant tout d'informer les personnes sur ce que vous faites de leurs données et de respecter leurs droits. En tant que responsable de traitement de données, ou en tant que sous-traitant, vous devez prendre des mesures pour garantir une utilisation de ces données respectueuse de la vie privée des personnes concernées.

La protection des données à caractère personnel et le respect de la vie privée sont des droits fondamentaux majeurs. Le Parlement européen a toujours insisté sur la nécessité de maintenir une approche équilibrée entre renforcement de la sécurité et sauvegarde des Droits de l'homme, notamment en ce qui concerne la protection des données et la vie privée. De nouvelles règles de l'Union relatives à la protection des données à caractère personnel, qui

renforcent les droits des citoyens et qui, à l'ère numérique, simplifient les règles que les entreprises doivent respecter sont entrées en vigueur en mai 2018.

Il s'agit donc, ici, de savoir comment peut-on protéger les données à caractères personnel ?

I. Régime légal des flux transfrontières de données selon la convention 108 et le protocole additionnel

Dès l'adoption des premières lois de protection des données dans les années 1970, les législateurs nationaux ont perçu le risque inhérent aux flux transfrontières de données et ont adopté des dispositions légales encadrant la communication internationale de données à caractère personnel ⁽¹⁾. Le régime adopté était différent d'un pays à l'autre. On distinguait les lois qui ne régissaient pas spécialement le transfert hors des frontières nationales de celles qui soumettaient le flux à un régime de déclaration préalable, voire d'autorisation. Dans un monde interdépendant et dans lequel l'échange d'informations joue un rôle fondamental, la recherche de solutions internationales s'est rapidement avérée nécessaire, notamment pour éviter l'érection de barrières qui loin d'être efficaces pouvaient freiner ou paralyser certaines activités transfrontières.⁽²⁾ Le Conseil Européen et l'OCDE allaient dans ce contexte jouer un rôle phare dans l'élaboration d'une réglementation internationale et dans l'harmonisation des législations nationales. Avec l'adoption de la directive 95/46/CE 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, l'Union européenne a contribué à renforcer l'harmonisation des législations nationales des Etats membres et à créer un espace permettant d'échanger des données sans considération de frontières.⁽³⁾

¹-Ouverte à la signature le 28 janvier 1981, la Convention fut le premier instrument international juridique contraignant dans le domaine de la protection des données. Aux termes de cette Convention, les parties doivent prendre les mesures nécessaires en droit interne pour en appliquer les principes afin d'assurer, sur leur territoire, le respect des droits fondamentaux de la personne humaine au regard de l'application de la protection des données, Série des traités européens - n°108.

²-La décision-cadre 2008/977/JAI du Conseil est entrée en vigueur en mai 2018. Elle protège le droit des citoyens à la protection de leurs données à caractère personnel lorsque celles-ci sont utilisées par les autorités répressives, La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») a été modifiée par la directive 2009/136/CE du 25 novembre 2009.

³-Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

1.1-La Convention du Conseil Européen pour la protection des personnes à l'égard du traitement automatisé des données

a- Le but de la Convention

La Convention du Conseil Européen pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été ratifiée par 29 Etats membres. La Convention s'articule autour de trois axes :

- les principes de base de la protection des données qui doivent être transposés en droit interne ;
- la réglementation des flux transfrontières de données ;
- la coopération entre les parties.⁽⁴⁾

La Convention a pour objectif de concilier le droit au respect à la vie privée et la liberté d'information, notamment le droit à la libre circulation des données sans considération de frontières, libertés fondamentales énoncées à la convention européenne des droits de l'homme. Elle tend également à faciliter l'entraide internationale dans le domaine de la protection des données, limiter les risques de détournement des législations nationales, assurer l'équivalence de traitement entre nationaux et étrangers, encourager l'harmonisation des standards nationaux au bénéfice des personnes concernées et des responsables de traitement, faciliter la communication internationale des données.

b-Flux transfrontières de données

Conscient des risques inhérents aux flux transfrontières de données, notamment lorsque le transfert se fait vers un destinataire n'assurant pas un niveau de protection de données conforme aux exigences de la Convention, les

personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) est entré en vigueur en mai 2018, Le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE, est entré en vigueur le 11 décembre 2018.

⁴-La nouvelle proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») est en cours d'examen, voir : Jean-Philippe WALTER, « Défis posés par les flux transfrontières de données à caractère personnel », Council of EUROPE, www.coe.int/dataprotection, 2004, p.7.

auteurs de la Convention ont prévu une disposition particulière qui règle spécifiquement la communication transfrontière ou internationale de données. Cette disposition repose sur le principe selon lequel il ne devrait pas y avoir de communications transfrontières de données en l'absence d'un niveau de protection des données équivalent à celui du pays d'exportation des données. La Convention ne donne pas de définition de la protection équivalente, à savoir «*une protection dont l'effet est pour l'essentiel semblable à celle du pays exportateur mais qui ne doit pas nécessairement être identique à celle-ci, ni dans la forme, ni à tous autres égards*». ⁽⁵⁾

La Convention régit non seulement le transfert automatisé des données au-delà des frontières nationales, mais également d'autres types de transferts «*quel que soit le support utilisé*» de données à caractère personnel faisant l'objet d'un tel traitement ou destinées à un tel traitement. ⁽⁶⁾ La disposition couvre également la collecte de données par-dessus les frontières, notamment celle effectuée par un opérateur internet par exemple lors de la visite d'un site par un utilisateur (cookies, etc.). Elle tient ainsi compte de tous les modes de transfert. La notion de «*flux transfrontière de données*» couvre toute action qui implique que des données échappent à la souveraineté d'un Etat pour être traitées dans un autre Etat ou organisation. Elle nécessite au minimum que deux ordres juridiques différents soient touchés. La notion contient trois éléments importants

- des données à caractère personnel font l'objet d'un traitement ou sont destinées à un tel traitement ;
- les données sont transférées ;
- celui qui communique et le destinataire sont régis par des ordres juridiques différents. ⁽⁷⁾

L'article 12 de la Convention contient deux exceptions aux libres flux des données entre Etats contractants. La première exception permet, tout d'abord, de soumettre à des conditions restrictives la communication transfrontière de données à caractère personnel lorsque la législation nationale prévoit une réglementation spécifique pour certaines catégories de données personnelles ou

⁵-Rosario DUASO CALÉS, « Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau », Thèse présentée à la Faculté des études supérieures en vue de l'obtention du grade de Docteur en droit de la Faculté de droit de l'Université de Montréal et Docteur en droit de l'Université Panthéon - Assas Paris II, Septembre, 2011, p.45 ; voir aussi Pierre KAYSER, « La protection de la vie privée par le droit », Paris, Éd. Economica, 1995, p. 462.

⁶-Art12 La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, op.cit.

⁷-Miyase CHRISTENSEN, « Facebook is watching you », Le Monde diplomatique, Manière de voir, Internet, révolution culturelle, 109, février-mars 2010, pp. 52, 55.

de fichiers automatisés en raison de la nature de ces données ou fichiers. Une telle restriction ne pourra se justifier que si le pays destinataire n'offre pas une protection équivalente pour ce type de traitement. Elle ne couvre pas l'ensemble des transferts de données personnelles vers ce destinataire. La restriction vise en particulier les données sensibles qui seraient assujetties à des garanties spéciales méconnues de l'Etat destinataire.⁽⁸⁾

La deuxième exception vise le cas où des données sont transférées vers un Etat non contractant en transitant par un Etat contractant. Dans ce cas, des restrictions peuvent être introduites pour empêcher que la législation de l'Etat d'où partent les données ne soit détournée.

1.2-Protocole additionnel

L'objectif poursuivi par ce protocole est de renforcer la mise en œuvre des principes contenus dans la Convention, en particulier pour tenir compte de l'augmentation croissante des flux transfrontières de données, notamment vers des destinataires établis dans un Etat non contractant.⁽⁹⁾

« ... l'effectivité de cette protection implique une harmonisation au niveau international, non seulement des principes fondamentaux de la protection des données mais également, dans une certaine mesure, des moyens de mettre en œuvre ces principes – dans un domaine en perpétuelle évolution et caractérisé par une très forte technicité – et des conditions dans lesquelles les transferts de données à caractère personnel peuvent être effectués à travers les frontières »⁽¹⁰⁾

a- Niveau de protection adéquat

En règle générale, le niveau de la protection doit être évalué au cas par cas et pour chaque transfert ou type de transfert. L'évaluation devrait prendre en considération l'ensemble des circonstances relatives au transfert et notamment : *« la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le pays d'origine et le pays de destination finale,*

⁸-Jean-Philippe WALTER, op.cit, p 20, la directive 95/46/CE (règlement général sur la protection des données), op.cit.

⁹-Allain BENSOUSSAN, « Les flux transfrontières de données personnelles », Juristendances et libertés, N°21, mai 2008, pp. 2-3. voir notamment la recommandation R (97) 5 sur la protection des données médicales, la Recommandation R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques et la Recommandation R (2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

¹⁰-Jacques CHEVALLIER, « L'État post moderne », Paris, LGDJ, 2004, p.41 ; La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, op.cit.

les règles de droit, générales et sectorielles applicables dans l'Etat ou l'organisation en question et les règles professionnelles et de sécurité qui y sont respectées».⁽¹¹⁾

b-Dérogations

En l'absence d'un niveau de protection des données jugé adéquat, le transfert de données à caractère personnel vers un pays tiers devrait être prohibé. Le protocole additionnel prévoit cependant des dérogations. Ainsi, le transfert peut être autorisé si le droit interne de l'Etat contractant d'où les données devraient être communiquées, le prévoit pour des intérêts spécifiques de la personne concernée ou pour des intérêts légitimes, notamment des intérêts publics importants, prévalant les intérêts de la personne concernée. Ces exceptions devraient couvrir des cas d'espèce et non pas légitimer la communication régulière et systématique de données vers des Etats tiers n'offrant pas de garanties suffisantes pour le respect de la vie privée. Le transfert est également possible « *si des garanties pouvant notamment résulté de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne* ». ⁽¹²⁾ Ces garanties peuvent notamment découler des clauses contractuelles incluant les éléments pertinents de la protection des données et notamment préserver les droits des personnes concernées.

Toutefois la marge de manœuvre doit demeurer étroite. « *Les règles pertinentes de droit interne doivent néanmoins respecter le principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle. Cet intérêt peut être de protéger un intérêt public important, tel que défini dans le contexte de la Convention européenne des droits de l'homme et de la Convention 108 ; l'exercice ou la défense d'un droit en justice ; ou lorsqu'il s'agit de données extraites d'un registre public. Des exceptions peuvent également être prévues pour répondre à des intérêts spécifiques de la personne concernée, pour l'exécution d'un contrat conclu avec la personne concernée ou*

¹¹-loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, JR N°182 du 7 août 2004. Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, Série des traités européens - n° 181,2001. Art. 3 chiffres 4 et 5 de la Convention.

¹²-Article 25 et 31 de la directive 95/46/CE, Y. Pouillet, Pour une justification des articles 4, 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données.

europa.eu.int/comm/internal_market/en/dataprot/lawreport/speeches/pouillet_fr.pdf

dans l'intérêt de celle-ci, pour la protection de ses intérêts vitaux ou lorsqu'elle a donné son consentement. Dans ce cas, avant de consentir, la personne concernée doit être informée de manière appropriée du transfert envisagé.»⁽¹³⁾

2-Réglementations des flux transfrontières au niveau national

La plupart des lois nationales de protection des données des Etats parties à la Convention 108 contiennent des dispositions particulières régissant les flux transfrontières de données soumettant le transfert des données au-delà des frontières nationales au respect de conditions spécifiques. En plus de ces conditions spécifiques, le préalable au transfert est que le traitement des données et leur communication respectent les autres conditions légales et notamment les principes de base de la protection des données de la Convention.

Du fait de la directive européenne et dans une certaine mesure du protocole additionnel à la Convention 108, ces réglementations nationales ont un point commun : le transfert est en règle générale possible si le destinataire des données est soumis à un régime de protection des données assurant un niveau de protection adéquat. Le transfert vers des pays n'assurant pas un niveau de protection adéquat est également possible dans certaines circonstances et moyennant le respect de conditions déterminées. Le système de la notification ou de l'autorisation préalable sont encore bien implantés. L'approche contractuelle est également retenue dans la plupart des législations.⁽¹⁴⁾

3-Rôle des autorités de protection des données

Les tâches des autorités de protection des données en matière de flux transfrontières de données sont définies dans les lois nationales, à la lumière de l'examen de différentes lois nationales, nous pouvons recenser les tâches et compétences qui sont celles plus ou moins de l'ensemble des autorités, à savoir :

- Examen des notifications ou déclarations de transfert avec dans certains pays l'enregistrement de la notification dans le registre des traitements, voire la délivrance d'une autorisation de transfert ;
- Investigation sur la conformité aux exigences légales avec le cas échéant exercice des pouvoirs d'intervention dévolus à l'autorité (recommandation,

¹³-Nicolas Tilli, « La protection des données à caractère personnel », Documentaliste-Sciences de l'Information V50, N°3, 2013, pp. 62 à 69.

¹⁴-Article 2 al 2 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, n° 108 du 28 janvier 1981 ; Voir aussi : - Décisions DC 83-164 de 1983, DC 84-184 de 1984, DC 90-281 de 1990, DC 93-316 de 1993, DC 95-352 de 1995, DC 96-377 de 1996 et DC 97-389 de 1997.

décision et parfois sanction ou dénonciation à l'autorité judiciaire compétente)⁽¹⁵⁾ ;

-Evaluation du niveau adéquat de protection de cas en cas et/ou de manière générale, avec dans certains Etats l'établissement d'une liste des Etats dotés d'une législation de protection des données garantissant ce niveau de protection des données adéquat ;

-Examen des clauses contractuelles ou d'autres garanties propres à assurer la protection des droits des personnes concernées ;

-Adoption de recommandations générales ou d'instructions (avec parfois une valeur normative) ;

-Information des personnes concernées sur leurs droits ;

-Information des responsables de traitement sur leurs obligations ;

-Collaboration avec les autorités de protection des données d'autres Etats, notamment conformément aux articles de la Convention 108 et du Protocole additionnel.⁽¹⁶⁾

II. La protection des données personnelles en Algérie

La présente loi a pour objet de fixer les règles de protection des personnes physiques dans le traitement des données à caractère personnel ; le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, doit se faire dans le cadre du respect de la dignité humaine, de la vie privée, des libertés publiques et ne doit pas porter atteinte aux droits des personnes, à leur honneur et à leur réputation.⁽¹⁷⁾ La Loi n°18-07 va donc régir ce qui s'échange sur Internet comme données à caractère personnel. Quelles sont les grandes lignes que comporte la loi relative à la protection des données à caractère personnel ?

•Grandement inspiré par les législations tunisienne et belge en la matière, selon une source du ministère de la Justice (la première ébauche eut été esquissée par le ministère des TIC).

•Le document spécifie ce qu'il est entendu par son propos : « *La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données à caractère personnel [...] Elle veille à ce*

¹⁵-Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre. La directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens,

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf

¹⁶-Directive n° 95/46/CE du 24 octobre 1995.

¹⁷-Art.1 et 2 de la loi n°18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JO n° 34, 2018-06-10.

que les technologies de l'information et de la communication ne portent pas atteinte aux libertés individuelles ou publiques, notamment à la vie privée. »⁽¹⁸⁾

A-Naissance de l'ANPDCP

La loi sur la protection des données personnelles signe l'acte de naissance d'une autorité nationale appelée à devenir l'unique interlocuteur de toute personne concernée par la collecte, le traitement ou encore le stockage de ces données et c'est également le seul vis-à-vis des utilisateurs que nous sommes. En vertu de cette loi, « *il est institué une Autorité nationale de protection des données à caractère personnel* ». Elle est dotée du statut juridique d'une autorité administrative indépendante et son budget inscrit sur celui de l'Etat.⁽¹⁹⁾

B-Composition de l'organigramme de l'ANPDCP

Celui-ci est constitué d'un président, un membre de l'Assemblée populaire nationale, un autre encore mais issu du Conseil de la nation, un représentant du Premier ministre, de deux magistrats de la Cour suprême ; deux autres du Conseil d'Etat, puis un seul représentant des ministères de l'Intérieur, de la Défense nationale, de la Justice, de la Poste et des TIC et enfin un chercheur du ministère de la Recherche scientifique,⁽²⁰⁾ un médecin pour représenter son

¹⁸-**Données à caractère personnel** : « *toute information, quel qu'en soit son support, concernant une personne identifiée ou identifiable, ci-dessous dénommée « personne concernée», d'une manière directe ou indirecte, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale* » ; art.3 de loi n°18-07 du 10 juin 2018, op.cit.

¹⁹-Art.12 de la loi 18-07op.cit : « *Nonobstant toute disposition législative contraire, toute opération de traitement des données à caractère personnel, est soumise à une déclaration préalable à l'autorité nationale ou à son autorisation conformément aux dispositions prévues par la présente loi* », art. 22 de la loi 18-07 op.cit : « *Il est créé, auprès du Président de la République, une autorité administrative indépendante de protection des données à caractère personnel, désignée ci-après « l'autorité nationale », dont le siège est fixé à Alger. L'autorité nationale jouit de la personnalité morale et de l'autonomie financière et administrative. Le budget de l'autorité nationale est inscrit au budget de l'Etat. Il est soumis au contrôle financier conformément à la législation en vigueur. L'autorité nationale élabore et adopte son règlement intérieur qui fixe notamment les modalités de son organisation et son fonctionnement* ».

²⁰-Art. 23 de la loi 18-07, op.cit : « *L'autorité nationale, est composée de : -trois (3) personnalités dont le président, choisies par le Président de la République en raison de leurs compétences dans le domaine d'activité de l'autorité nationale ; - trois (3) magistrats, proposés par le Conseil supérieur de la magistrature, parmi les magistrats de la Cour suprême et du Conseil d'Etat ; -un (1) membre de chacune des chambres du Parlement*

ministère de tutelle et un membre de la Commission nationale pour les droits de l'homme. La liste ne semble pas définitivement close. Autant le président que les membres seront désignés par décret présidentiel et siégeront dans cette autorité pour une période de 05 ans.

C-Missions de l'ANPDCP

L'Autorité a pour mission d'« *accorder les autorisations, recevoir les déclarations pour la mise en œuvre du traitement des données à caractère personnel ou les retirer dans les cas prévus par la loi, de recevoir les plaintes portées dans le cadre de la compétence qui lui est attribuée, accéder aux données à caractère personnel faisant l'objet d'un traitement afin de procéder à leur vérification, élaborer des règles de conduite relatives au traitement* » de ces mêmes données. Comme autre attribution, celle l'autorisant à « *procéder aux investigations requises en recueillant les déclarations de toute personne dont l'audition est jugée utile et en ordonnant de procéder à des constatations dans les locaux et lieux où a eu lieu le traitement à l'exception des espaces d'habitation* ». Sur ce dernier point précisément, que les professionnels qui sont concernés de près ou de loin par la collecte et le traitement des données à caractère personnel sachent qu'ils ne peuvent en aucun cas « apposer » à l'autorité nationale le sacro-saint principe du « secret professionnel ». ⁽²¹⁾

-Contenu

Le document dédie toute une section à des généralités qui reviennent sur l'ensemble des aspects liés aux données à caractère personnel. Cela va du cadre dans lequel cette donnée est collectée, comment elle est traitée et à quelle fin de même que les procédures liées à son stockage. La section qui suit consacre, pour

choisis par leurs présidents, après consultation des présidents des groupes parlementaires ; - un (1) représentant du Conseil national des droits de l'Homme ; - un (1) représentant du ministre de la défense nationale ; -un (1) représentant du ministre des affaires étrangères ; - un (1) représentant du ministre chargé de l'intérieur ; - un (1) représentant du ministre de la justice, garde des sceaux un (1) représentant du ministre chargé de la poste, des télécommunications, des technologies et du numérique ; -un (1) représentant du ministre chargé de la santé ; -un (1) représentant du ministre du travail, de l'emploi et de la sécurité sociale. Les membres de l'autorité nationale sont choisis, en raison de leur compétence juridique et/ou technique dans le domaine du traitement des données à caractère personnel. L'autorité nationale peut faire appel à toute personne compétente susceptible de l'aider dans ses travaux. Le président et les membres de l'autorité nationale sont désignés par décret présidentiel pour un mandat de cinq (5)ans renouvelable ».

²¹-Art.5 et 25 de la loi 18-07, op.cit.

sa part, le « principe de consentement » et surtout celui de se rétracter et de demander jusqu'à la suppression de ces données par l'utilisateur bien sûr. Evidemment, en adressant la demande à l'autorité nationale qui prendra le relais.⁽²²⁾

-Cas prospection directe

Elle concerne la réorganisation de l'activité de la prospection directe. Il est écrit : « *Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique ou d'un moyen employant une technologie de même nature qui utilise, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.* ». Alors, au sens de cet de loi, constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une personne vendant des biens ou fournissant des services⁽²³⁾.

D'après ce document, ne sont pas concernées, selon toute vraisemblance, les prospections « business-to-business ». En ce qui concerne la prospection directe via le courrier électronique, elle est autorisée dans le cas où les coordonnées du destinataire auraient été récoltées directement auprès de lui lors d'une vente ou d'une prestation de service sous réserve que lui soit accordée de manière explicite la possibilité de s'opposer à l'utilisation de ses coordonnées pour des prospections à l'égard des tiers. Dans tous les cas de figure, il ne sera plus possible aux opérateurs économique dont l'activité repose en partie ou en totalité sur la prospection directe de le faire sans qu'il soit indiqué une coordonnée valable à laquelle le prospect pourrait se référer pour demander et obtenir que la communication cesse.⁽²⁴⁾

Le traitement de ces données doit faire l'objet soit d'une autorisation préalable, soit d'une déclaration simplifiée. Evidemment, tout se passe et se passera au niveau de l'Autorité nationale qui spécifiera quelles données seront sous l'un ou l'autre régime. Toutefois, les données à caractère sensible, c'est-à-dire toute information dite de « souveraineté », comprendre les données récoltées pour la constitution d'un document administratif –carte d'identité, passeport, permis, etc.- sont l'exclusivité de l'autorité publique, donc de l'Etat.

²²-Art. 32 de la loi 18-07, op.cit.

²³-BENCHAREF (CH), « De la nécessité pour les Algériens de protéger leurs données personnelles », EL WATAN.com, 03-11-2019, p. 3.

²⁴-Art.33 de loi n°18-07 op.cit.

D-Protection des données personnelles sur les réseaux sociaux (Facebook et autres)

Qu'en est-il ou qu'en sera-t-il des données à caractère personnel qui circulent sur les réseaux sociaux, Facebook en premier, le document spécifie : « *En cas de collecte de données en réseaux ouverts, la personne concernée doit être informée, sauf si elle sait déjà que les données personnelles la concernant peuvent circuler sur les réseaux sans garantie de sécurité et qu'elles risquent d'être lues et utilisées par des tiers non autorisés* ». Le document ne mentionne pas quelle est la démarche à suivre si jamais des données personnelles d'un utilisateur circulent sur les réseaux à son insu ou sont carrément utilisées par des tiers non autorisés. Peut-il recourir à l'autorité nationale qui diligente une procédure afin de l'assister ? Pas de réponse.⁽²⁵⁾

Qu'en est-il ou qu'en sera-t-il de ceux qui manipulent des données personnelles mais les hébergent dans des serveurs à l'étranger, la réponse est apportée par le « chapitre dédié au transfert de données vers un pays étranger ». L'article qui le concerne stipule : « *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat étranger que si cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet* ». Encore que, il faut attendre que l'autorité nationale établisse la liste des Etats répondant à ces critères.⁽²⁶⁾

²⁵-Marie De Fournas, «Réseaux sociaux: Comment concilier protection des données personnelles et popularité? », le journal de 20 Minutes, 27/08/18, p.7. Voir aussi art.7 de la loi n°18-07 op.cit.

²⁶-Art. 4 de la loi 18-07, op.cit. : « *La présente loi s'applique au traitement automatisé en tout ou en partie des données à caractère personnel, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans des fichiers manuels. La présente loi s'applique au traitement des données à caractère personnel effectué par des organismes publics ou des personnes privées : 1- lorsqu'il est effectué par une personne physique ou morale dont le responsable est établi sur le territoire algérien ou sur le territoire d'un Etat dont la législation est reconnue équivalente à la législation nationale en matière de protection des données à caractère personnel. Est considéré comme établi en Algérie, le responsable d'un traitement qui exerce une activité sur le territoire algérien dans le cadre d'une installation, quelle que soit sa forme juridique ; 2- lorsque le responsable n'est pas établi sur le territoire algérien mais recourt, à des fins de traitement des données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire algérien, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire national. Dans ce cas, le responsable du traitement doit notifier à l'autorité nationale, l'identité de son représentant installé en Algérie qui, sans préjudice de sa responsabilité personnelle, se substitue à lui dans tous ses droits et obligations résultant des dispositions de la présente loi et des textes pris pour son application* ».

Enfin, beaucoup d'aspects liés à la vie privée ne sont pas pris en compte. Parmi ces problématiques, le GPS rentre-t-il dans la catégorie donnée à caractère personnel ? Les applications qui ont accès aux données d'identification sont-elles concernées ? Le droit à l'image, ces images que récupèrent les systèmes de vidéosurveillance ? Et le fameux « Cloud » dans tout ça ? Ce ne sont pas les seules questions sachant que ce qui est lié aux nouvelles technologies de l'information et de la communication évolue très vite. De plus en plus ; tous les équipements se recourent, et c'est une tendance très forte, au point que le champ d'application doit viser de façon neutre tous les environnements à partir desquels nous nous connectons pour échanger nos données – tablettes, Smartphones, téléviseurs.

2-Globalisation de l'information

La globalisation de l'information, le développement des échanges et du commerce international, la mobilité croissante (volontaire ou contrainte) des personnes, les exigences économiques, la pression sur les coûts, ainsi que les exigences de rationalisation entraînent une augmentation considérable des flux transfrontières de données à caractère personnel, une densification des réseaux de communication et une accélération massive des échanges d'information. Les échanges internationaux de données à caractère personnel ne sont ainsi pas seulement une réalité et une nécessité pour les activités des entreprises internationales (notamment gestion des données du personnel ou des clients). Ils touchent également l'ensemble des activités dépassant le cadre régional ou national (entraide administrative ou judiciaire internationale, tourisme, commerce électronique, recherche scientifique, etc.).⁽²⁷⁾

Ainsi, avec l'informatisation des relations de production et des rapports commerciaux, les données personnelles ne restent pas dans une entreprise ou dans un groupe d'entreprises. Elles sont également transmises à des partenaires commerciaux à l'étranger, enregistrées dans des banques de données internationales ou dans des centres de calculs en réseau dans le cadre notamment d'opérations d'outsourcing gérées par des prestataires de services actifs au niveau mondial. Le succès et la généralisation de l'Internet crée un espace accessible au grand public et aux marchands qui relie des centaines de millions d'utilisateurs échangeant des masses d'informations.⁽²⁸⁾

²⁷-Le transfert a lieu vers un pays reconnu par la Commission européenne comme "adéquat". C'est le cas du Canada, de la Suisse, de l'Argentine, des territoires de Guernesey, de Jersey et de l'Isle de Man. Cette liste évolue et peut être consultée sur le site de la CNIL (www.cnil.fr).

²⁸-Tristan Mattelart, « Les enjeux de la circulation internationale de l'information », Revue française en sciences de l'information et de la communication, N°17,2019, p.18.

A l'ère de la globalisation et de l'internationalisation des échanges, le traitement des données à caractère personnel ne connaît plus de frontières et la technologie rend de plus en plus facile la dissémination ou la délocalisation des traitements.

Enfin le phénomène Internet génère une production de données qui peuvent être utilisées à des fins diverses par des multitudes d'acteurs à travers le monde sans que la personne concernée ait réellement conscience de la portée des informations qu'elle met à disposition de manière plus ou moins librement accessible ou sans qu'elle sache qui collecte ou intercepte des informations à son égard (allusion notamment aux cookies ou autres mouchards informatiques qui permettent notamment de sélectionner les messages publicitaires à envoyer aux internautes et de profiler ou de contrôler les utilisateurs).⁽²⁹⁾

3. Défi envers la protection des données

Cette globalisation de la société et des échanges d'informations sans considération de frontières constitue un défi redoutable pour la protection des données (la vie privée) et les autorités chargées de veiller au respect des dispositions légales. Le monde se partage entre les pays qui ont encadré le traitement de données personnelles par une législation, c'est le cas de la majorité des pays membres du Conseil de l'Europe, de ceux qui, sans nier la nécessité d'une protection, estiment à l'instar des Etats-Unis qu'il revient au marché de s'autoréguler et de ceux qui ignorent le problème. Les personnes concernées et les autorités de contrôle se voient ainsi démunies du fait de la perte de maîtrise sur les données qui échappent lors de leur transfert aux dispositions nationales de protection des données. Il est dès lors important que les flux transfrontières de données à caractère personnel soient encadrés et que les autorités de protection des données soient en mesure de veiller à ce que les principes de la protection des données soient pris en compte lors de transferts pour garantir le respect de la vie privée des individus et des droits qui en découlent.⁽³⁰⁾

²⁹-ibidem, p. 26 ; Art. 32 de la loi 18-07, op.cit. « *Sauf si elle en a déjà eu connaissance, toute personne sollicitée, en vue d'une collecte de ses données à caractère personnel, doit être, préalablement, informée de manière expresse et non équivoque par le responsable du traitement ou son représentant, des éléments suivants :- l'identité du responsable du traitement et, le cas échéant, de son représentant ;- les finalités du traitement ;- toutes informations supplémentaires utiles notamment le destinataire, l'obligation de répondre et ses conséquences.* »

³⁰-NKINGI (D), « Autoroutes de l'information et la mondialisation », revue Hermes N°2, 2006, p.99.

4. Aspects internationaux de la protection des données individuelles et des banques de données

L'accroissement considérable des flux de données à travers les frontières nationales et la création de banques internationales de données (collections de données destinées à être extraites et à d'autres fins) ont mis en évidence la nécessité d'une action nationale concertée, tout en venant étayer les arguments en faveur de la libre circulation de l'information, qui doit souvent être considérée en regard des exigences liées à la protection des données et des limitations imposées à la collecte, au traitement et à la diffusion de ces données.⁽³¹⁾

A l'échelon international, on se préoccupe avant tout de parvenir à un consensus au sujet des principes fondamentaux sur lesquels doit reposer la protection des personnes physiques. Un tel consensus supprimerait ou diminuerait les raisons de réglementer l'exportation des données et faciliterait la solution des problèmes soulevés par les conflits de loi. En outre, il pourrait marquer un premier pas sur la voie de l'élaboration d'accords internationaux plus détaillés ayant force exécutoire.⁽³²⁾

Il y a d'autres raisons pour lesquelles la réglementation du traitement des données de caractère personnel devrait être envisagée dans un contexte international : les principes en jeu concernent des valeurs que de nombreux pays sont très soucieux de sauvegarder et de voir généralement acceptées ; ils peuvent aider à réaliser des économies sur les coûts afférents à la circulation internationale de l'information. Il est de l'intérêt commun des pays d'empêcher la constitution d'enclaves dans lesquelles on pourrait facilement se soustraire aux règlements nationaux en matière de traitement de l'information; en fait, compte tenu de la mobilité internationale des individus, des biens et des activités commerciales et scientifiques, des pratiques acceptées d'un commun accord eu égard au traitement des données peuvent comporter des avantages, même lorsque la circulation de l'information à travers les frontières n'est pas directement en cause.⁽³³⁾

Qu'est-ce qu'un transfert de données à caractère personnel ?

On parle de transfert de données personnelles lorsque les données personnelles sont transférées depuis le territoire européen vers un ou des pays

³¹-Jean-Philippe WALTER, op.cit, p.40.

³²-Tristan Mattelart, op.cit, p.23.

³³-Selon l'article 52 de la loi 18-07 op.cit. « Le titulaire d'un droit au titre de la présente loi, qui prétend être lésé par son atteinte, peut demander à la juridiction compétente toutes mesures conservatoires tendant à faire cesser cet acte ou à l'octroi d'une réparation ».

situés hors de l'Union européenne. Le transfert peut s'effectuer, par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre (ex. d'un disque dur d'ordinateur à un serveur).

Quelles dispositions régissent les transferts de données à caractère personnel en France ?

-Loi « Informatique et Libertés » relative à l'informatique et aux libertés.

Le principe est posé par la loi : les transferts en dehors de l'Union européenne sont interdits.

Les exceptions sont prévues par la loi :

Les transferts en dehors de l'Union européenne sont autorisés si le pays ou l'entreprise destinataire assure un niveau de protection adéquat aux données transférées. Cette protection adéquate peut être apportée de plusieurs manières :

-Légalement, si le pays destinataire des données personnelles a une législation reconnue par la Commission européenne comme offrant une protection adéquate. C'est le cas du Canada, de l'Isle de Man, de la Suisse, de l'Argentine, de Guernesey et de Jersey, ou

-De manière contractuelle, par la signature de Clauses Contractuelles Types adoptées par la Commission européenne entre l'entité exportatrice et l'entité importatrice de données personnelles, ou par l'adoption de Règles internes d'entreprise ou BCR (BINDING CORPORATE RULES) qui constituent un code de conduite en matière de transferts de données personnelles depuis l'Union européenne vers des pays tiers, ou

-Lorsque l'entité importatrice est basée aux Etats-Unis et qu'elle adhère au principe de Safe Harbor.

-L'article 69 permet également d'opérer des transferts dans des situations exceptionnelles.

Exemple 1 - Une entreprise souhaite sous-traiter la gestion des relances téléphoniques de ses clients à une société située dans un pays situé hors de l'Union européenne.

Exemple 2 - Les données des salariés d'une multinationale sont centralisées par la maison mère située aux Etats-Unis. Les données personnelles des salariés français font donc l'objet d'un transfert vers les Etats-Unis.

Comment encadrer les transferts de données ?

Pour que les transferts hors de l'Union européenne soient autorisés, il faut que le pays ou l'entreprise destinataire assure un niveau de protection adéquat aux données transférées. C'est le cas lorsque :

-le transfert a lieu vers un pays reconnu par la Commission européenne comme "adéquat". C'est le cas du Canada, de la Suisse, de l'Argentine, des territoires de Guernesey, de Jersey et de l'Isle de Man. Cette liste évolue et peut être consultée sur le site de la CNIL (www.cnil.fr). ou

-des Clauses Contractuelles Types de la Commission Européenne sont signées entre deux entreprises, ou

-des Règles internes d'entreprises (BCR) sont adoptées au sein d'un groupe, ou l'entreprise destinataire est située aux Etats-Unis et adhère au Safe Harbor, ou des exceptions de la loi Informatique et Libertés peuvent être invoquées.

Existe-t-il d'autres règles à respecter dans le cadre d'un transfert de données ?

Un transfert de données hors Union européenne, comme une communication de données à un tiers sur le territoire français, constitue un traitement de données à caractère personnel. Il est soumis à ce titre à l'ensemble des dispositions de la loi « Informatique et Libertés ».

-Tout transfert de données vers l'étranger doit avoir une finalité déterminée, explicite et légitime ;

-Les données transférées ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité ;

-Les données transférées doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités pour lesquelles elles sont transférées ;

-Les personnes dont les données doivent être transférées doivent être informées de l'existence de ce transfert ;

-La durée de conservation des données transférées ne doit pas être excessive ;

-Les personnes doivent se voir garantir un droit d'accès et un droit de rectification en ce qui concerne les données transférées, ainsi qu'un droit d'opposition aux transferts ;

-Des mesures techniques de sécurité doivent être mises en place afin de protéger les données contre tout accès ou toute destruction, altération ou diffusion non autorisée desdites données.

Transférer des données personnelles pour une finalité différente que celle pour laquelle les données ont été initialement collectées. La loi informatique et libertés prévoit expressément que les données doivent être collectées pour une finalité déterminée. Elles ne doivent pas être réutilisées pour des finalités incompatibles avec les finalités initiales, à moins que la législation ne l'exige. En conséquence, tout transfert de données hors de l'Union européenne pour une finalité incompatible avec celle pour laquelle les données ont été initialement collectées est illégal. Tout nouveau transfert de données personnelles pour une nouvelle finalité doit être expressément autorisé par la CNIL.⁽³⁴⁾

³⁴-Art 64 de la loi n°18-07, op.cit, « Est puni d'un emprisonnement de deux (2) mois à deux (2) ans et d'une amende de 20.000 DA à 200.000 DA ou de l'une de ces deux peines seulement, tout responsable de traitement qui refuse, sans motif légitime, les droits d'information, d'accès, de rectification ou d'opposition prévus aux articles 32, 34, 35 et 36 de la présente loi. », Art 65 de la loi n°18-07, op.cit, « Sans préjudice des peines plus graves prévues par la législation en vigueur, toute violation, par le responsable du traitement, des obligations prescrites aux articles 38 et 39 de la présente loi, est punie d'une amende de 200.000 DA à 500.000

Informers les personnes concernées lorsque je transfère leurs données vers un pays tiers. Afin de garantir un traitement légitime des données personnelles, les responsables de traitement doivent informer les personnes concernées, avant tout transfert, de ce que leurs données feront l'objet d'un transfert vers un pays tiers. Les personnes concernées doivent notamment être informées de la finalité du transfert, du ou des pays destinataires, de la nature des données transférées, de la ou des catégories de destinataires, et du niveau de protection offert par le pays destinataires.

Quelles sanctions encourt le responsable de traitement en cas de non-respect des règles en matière de transferts ?

Les sanctions pénales en cas de non-respect des règles en matière de transferts peuvent aller de 300 000 euros d'amende à 5 ans d'emprisonnement (Code pénal).

Par ailleurs, la CNIL dispose également de pouvoirs propres de sanction. Ainsi, aux termes de l'article 45, la CNIL peut :

- prononcer un avertissement à l'égard du responsable de traitement qui ne respecterait pas les obligations découlant de la présente loi,
- mettre en demeure de faire cesser le manquement constaté dans un délai qu'elle fixe.

Après une mise en demeure, la Commission peut également prononcer à l'encontre du responsable de traitement :

- une sanction pécuniaire (allant de 150 000 euros pour le premier manquement à 300 000 euros en cas de manquements réitérés ou 5% du chiffre d'affaires dans la limite de 300 000 euros pour les entreprises)
- une injonction de cesser le traitement ou un retrait de l'autorisation accordée par la CNIL.

Qu'entend-on par « destinataire de données » ?

Le destinataire de données est celui vers lequel les données à caractère personnel sont exportées. Il peut s'agir d'un responsable de traitement ou d'un sous-traitant.⁽³⁵⁾

DA. Est puni des mêmes peines quiconque conserve des données à caractère personnel au-delà de la durée prévue par la législation en vigueur ou de celle prévue dans la déclaration ou l'autorisation. », voir aussi Art 66 « Le fait pour un fournisseur de services de ne pas procéder à la notification d'une violation de données à caractère personnel à l'autorité nationale ou à l'intéressé, en méconnaissance des dispositions de l'article 43 de la présente loi, est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 100.000 DA à 300.000 DA ou de l'une de ces deux peines seulement. »

³⁵-Art 54 de la loi n°18-07, op.cit, « Sans préjudice des peines plus graves prévues par la législation en vigueur, est punie d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 200.000 DA à 500.000 DA, la violation des dispositions de l'article 2 de la présente loi. », Art. 55 de la loi 18-07 op.cit, « Quiconque procède à un traitement de

Conclusion

Même si en l'absence d'une réglementation de protection des données déployant ses effets au-delà du continent européen, il est possible et nécessaire de trouver un rattachement au territoire national pour l'ensemble ou du moins une grande majorité des flux transfrontières de données issus de ce territoire et ainsi de pouvoir sanctionner les violations de nos dispositions légales.

L'action des autorités nationales de protection des données doit ainsi s'attacher à sensibiliser les personnes concernées et les responsables de traitement aux risques liés aux flux transfrontières de données. Cela passe par :

- une politique d'information active,
- une évaluation des risques et l'élaboration d'« outils » pour permettre de réaliser les exigences de la protection des données et diminuer les risques d'atteinte aux droits des personnes concernées,
- un contrôle et le cas échéant la prise de sanctions,
- une intensification de la collaboration internationale.

données à caractère personnel, en violation des dispositions de l'article 7 de la présente loi, est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 100.000 DA à 300.000 DA. Est puni des mêmes peines quiconque procède à un traitement de données à caractère personnel malgré l'opposition de la personne concernée, lorsque ce traitement répond à des fins notamment, de prospection commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes. »