Journal of letters and Social Sciences (JLSS) مجلة الآداب والعلوم الاجتماعية
https://www.asjp.cerist.dz/en/PresentationRevue/4

Protection des données à caractère personnel : Un cadre juridique en évolution

Protection of Personal Data: An Evolving Legal Framework

Dr. Wassila Kannoufi
د. وسيلة قنوفي
Université Mohamed Lamine Debaghine Sétif2, Algerie
cristalll_19@yahoo.fr

Informations sur l'article
Date de réception: 16/01/2020
Date d'acceptation:15/06/2021

Mots clés
Données personnelles
traitement des données personnelles
concerné par le traitement
responsable du traitement
règlement général

Résumé

L'avancée technologique qui s'est reflétée sur l'administration électronique dans la vie contemporaine l'a transformée en une arme à double tronchant, puisqu'elle a contribué d'une part à économiser l'effort, le temps ainsi que l'argent dans ses rapports avec ceux qui en sont bénéficiaires, mais elle a toutefois été à l'origine de l'apparition de risques touchant de manière directe la vie privée des individus; chose qui a nécessité de mettre en place un système juridique pour la protection des données à caractère personnel, au niveau international ainsi que sur le plan intérieur. Dans ce contexte, le législateur algérien n'a pas tardé à protéger cet aspect de la vie privée des individus au moyen de la loi 17/08 afin, qu'il y ait une concordance avec les législations internationals.

Introduction

Nous vivons dans un monde envahi par la technologie numérique, au point que la plupart de nos transactions sont enregistrées avec nos informations personnelles. Il est vrai que l'administration électronique a simplifié et développé ses relations avec ces administrés, en réduisant le temps, les efforts et la complexité des procédures. Mais cette évolution des technologies de l'information s'est accompagnée de nombreux risques qui ont affecté négativement la vie personnelle des individus. Ce qui a conduit à l'émergence d'un nouveau concept dans l'arène juridique, qui est la protection des données personnelles.

L'émergence de cette idée était directement liée au développement des technologies de l'information et à la concurrence des organisations et des entreprises dans l'acquisition électronique des logiciels, de collecte de données, afin de faciliter leurs transactions avec leurs clients. Tout cela a fait que les données personnelles ressemblent davantage à une marchandise demandée dans le monde virtuel.

Toutefois, les données à caractère personnel sont transmises en un tour de main au moyen de transactions électroniques quotidiennes, et parfois en raison des mauvaises intentions des internautes via le piratage, ou même de bonne foi de la part de la personne en question, sans en prendre conscience.

Mais ces fichiers utilisés par les administrations ne doivent pas pour autant constituer une source d'abus de pouvoir, ce qui rendrait nécessaire une évolution des règles régissant la protection des données a caractère personnel, et c'est la raison pour laquelle de nombreux textes réglementaires imposent à l'Etat, comme aux particuliers, des règles très contraignantes, lorsqu'il s'agit d'utiliser ces données. Cette protection a nécessité le besoin de dépasser la sphère locale, pour aller vers une protection internationale.

La présente étude essaie de répondre à la problématique suivante :

Quel est l'étendue de la compatibilité entre l'évolution dans le domaine juridique et l'évolution dans le domaine de la technologie associée au traitement des données à caractère personnel, tant au niveau national qu'international?

Afin de répondre à cette problématique nous proposons trois hypothèses principales :

-Le concept de « données à caractère personnel» en tant que nouveau concept nécessitant une protection juridique nous conduira inévitablement à étudier les concepts

qui lui sont associés dans le monde de l'administration électronique.

-La protection juridique des données à caractère personnel au niveau international a surement procédé la protection au niveau national.

-Le législateur algérien a certainement adopté les mêmes dispositions juridiques de la protection des données personnelles au niveau international.

Et pour cela, il convient donc de poser un cadre de réflexion qui permettrait d'étudier certains points essentiels de la protection des données à caractère personnel, afin de percevoir le mouvement systémique à l'œuvre, en adaptons une approche descriptive et analytique, et des fois comparatives, à cet égard Il est nécessaire de diviser cette étude en trois sections principales :

Section 1 : Le cadre conceptuel des données personnelles.

Section 2 : Le cadre juridique de la protection des données personnelles sur le plan international.

Section 3 : Le cadre juridique de la protection des données personnelles sur le plan national.

1–Le cadre conceptuel des données personnelles

«Les données à caractère personnel» est un nouveau concept résultant de l'utilisation croissante des technologies de l'information. Avant d'aborder la protection juridique de ce concept, nous devons d'abord définir un cadre conceptuel pour ce terme et les concepts les plus importants qui lui sont associés.

1–1–Définition des données personnelles

On entend par «données personnelles» ou «données à caractère personnel» toute information qui permet d'identifier les individus et qui, de ce fait, leur appartient **(**Chatillon 2016, 04) Le mot englais «privacy» est l'équivalent de l'expression «données personnelles». Privacy et données personnelles renvoient à ce qu'on appelle la vie privée, l'intimité des personnes, l'à côté de ce qui n'est pas public, ce qui ne regarde personne en dehors des intéressés eux-mêmes , dans le cadre du respect de l'ordre public et les bonnes mœurs, et ce qui doit être rigoureusement protégé par des barrières infranchissables , sous peine de commettre un délit civil, voire pénal (Braibant 1998, 08)

Le législateur français était le premier à donner une définition juridique aux données personnelles dans la Loi de 1978 « Informatique et Libertés » comme « toute information relative à une personne physique identifiée ,ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres » (Loi n° 78-17 s.d.)

L'union européenne aussi et a travers Le **règlement nº 2016/679**, dit **règlement général sur la protection des données** (Le règlement n°2016/679 2016) a adopté presque la même définition que le législateur français , dans l'article 4/1, et presque la même formulation en déclarant que : Aux fins du présent règlement, on entend par :

«données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable, (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne (Le règlement n°2016/679 2016)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 » (L'article 04 du Règlement no2016/679 2016)

Le législateur algérien a son tour donne une définition des données personnelles qui n'est pas très différente des définitions précédentes, et ca dans la **loi nº 18/07** du 10 juin 2018 **relative à la protection des personnes physiques dans le traitement des données à caractère personnel** , précisément dans l'article 03/1 , en déclarant que : « aux fins de la présente loi , on entend par « Données à caractère personnel » toute information quel qu'en soit son support, conservant 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 » (Loi N°18/07 2018)

Dans ce sens-là, et a travers ces définitions, on peut dire qu'une donnée personnelle est toute information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'un prénom, l'âge, le métier, une photo, l'adresse postale, l'adresse mail, le numéro de téléphone, la date de naissance, le numéro IP, une photographie, tout numéro d'identification, tel le «numéro d'inscription au répertoire» un identifiant de connexion informatique ,une empreinte digitale, un enregistrement vocal, des données de localisation, et tous «éléments spécifiques propres à son identité physique,

physiologique, générique, psychique, économique, culturelle ou sociale etc . (Le règlement n°2016/679 2016)

Les définitions précisent donc que pour déterminer si une personne est identifiable, il faut tenir compte de tous les moyens envisageables pour permettre son identification, tous ceux auxquels peut avoir accès le responsable du traitement, ou toute autre personne**,** fourni une liste des données pouvant être considérées comme personnelles, qu'elles soient seules ou associées à d'autres données :

-«Informations biographiques ou conditions de vie actuelles, y compris les dates de naissance, numéros de sécurité sociale, numéros de téléphone et adresses email.

-Apparences et comportements, y compris la couleur des yeux, le poids ou les traits de caractère.

-Informations professionnelles et liées à l'éducation, y compris le salaire, les données fiscales et numéro d'étudiant.

-Données privées et subjectives, y compris, la religion, les opinions politiques et les données de géolocalisation.

-Santé, maladie et génétique, y compris l'historique médical, les données génétiques et les informations liées aux congés maladie » (Meunier 2018)

1–2–Les concepts liés aux données personnelles

Plusieurs concepts sont étroitement liés au concept de données à caractère personnel, tels que le traitement des données, les données protégeables et l'accountability.

1–2–1–Qu'es qu'un traitement de données?

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles réalisées à l'aide de moyens , ou de procèdes automatisés , ou non (collecte, enregistrement, organisation, extraction ,conservation, adaptation, modification, consultation, utilisation, communication par transmission diffusion , ou toute autre forme de mise à disposition, rapprochement ou interconnexion ainsi que le verrouillage ou le cryptage, l'effacement ou la destruction des données). il est à retenir de tout cela , qu'un traitement de données personnelles n'est pas nécessairement informatisé, de ce fait les fichiers papiers sont également concernés , et par conséquent doivent être protégées dans les mêmes conditions. (L'article 04 du Règlement no2016/679 2016).

1–2–2–Qu'es qu'une donnée personnelle protégée?

Pour mieux comprendre la notion de données personnelles protégées, il faut préciser que toutes les données ne sont pas protégeables :

-Ce qui n'est pas protégeable (Quant aux personnes) :

La réglementation ne protège que les données qui concernent les personnes physiques, de ce fait les données permettant d'identifier les personnes morales, ne sont pas protégées par cette réglementation. En ce sens, les personnes morales ne peuvent pas jouir des droits prévus pour les personnes physiques, pour ce qui est du droit d'information quant à la finalité du traitement, du droit d'accès et d'opposition pour ne citer que ceux-ci, ce qui préserve en définitive le secret des affaires. (Caroline 2001)

-Ce qui n'est pas protégeable (Quant à la nature des données):

Certaines données ne relèvent pas du cadre de protection parce qu'elles ont été rendues anonymes et ne permettent pas l'identification de la personne.

1–2–3–Qu'est que «L'accountability»?

L'accountability (ou démontrabilité) désigne l'obligation pour les entreprises, de mettre en œuvre des mécanismes et des procédures internes , permettant de démontrer le respect des règles relatives à la protection des données . (Sma Faucheux 2018) La mise en œuvre du principe d'accountability implique la mise en place un ensemble de mesures internes , sous forme de mécanismes permettant de garantir le non atteint aux règles protectrices des données. Et pour cela, le principe d'accountability peut être atteint par :

-«La pseudonymisation et le cryptage des données personnelles, surtout si les données en cause sont sensibles (informations bancaires, condamnation, courant religieux…).

-La revue de la politique de confidentialité (analyse des systèmes de traitement des données, mesures pour limiter les risques de fuite…).

-La mise en place de procédure permettant de vérifier régulièrement l'efficacité des mesures de sécurité.

-L'inventaire des traitements.

-La désignation d'un DPO.

-La formation et la sensibilisation régulière du personnel au nouveau règlement sur la protection des données » (Accountability et règlement sur la protection des données personnelles 2018)

2–Le cadre juridique de la protection des données personnelles sur le plan international

En ce qui concerne la protection des données à l'échelon européen et/ou international, plusieurs textes doivent être pris en compte.

2–1–Au niveau de l'ONU

Le concept de vie privée, évoqué dès l'Antiquité, est présent depuis plusieurs centaines d'années dans différents textes de loi. Il a pris corps à partir de 1948, en étant inscrit au sein de l'article 12 de la Déclaration Universelle des Droits de l'Homme : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée (…). Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » (La Déclaration universelle des droits de l'homme (DUDH) s.d.)

Puis le Pacte international de l'ONU relatif aux droits civils et politiques (abrégé : Pacte ONU II) ne protège que la vie privée, sans mentionner la protection des données personnelles à son art 17 (Le pacte international relatif aux droits civils et politiques 1966) Qui reprend *in extenso* l'article 12 de la Déclaration des droits de l'Homme.

L'observation générale n°16 concernant cet article 17 du Pacte international, relatif aux droits civils et politiques, se réfère explicitement au droit à la protection des données à caractère personnel. Elle stipule spécifiquement que : « le rassemblement et la conservation, par des autorités publiques, des particuliers ou des organismes privés, de renseignements concernant la vie privée d'individus, sur des ordinateurs, dans des banques de données, et selon d'autres procédés, doivent être réglementés par la loi. L'État doit prendre des mesures efficaces, afin d'assurer que ces renseignements ne tombent pas entre les mains de personnes non autorisées par la loi, à les recevoir, les traiter et les exploiter, et ne soient jamais utilisés à des fins incompatibles avec le Pacte. Il serait souhaitable, pour assurer la protection la plus efficace de sa vie privée, que chaque individu ait le droit de déterminer, sous une forme intelligible, si des données personnelles le concernant et, dans l'affirmative, lesquelles, sont stockées dans des fichiers automatiques de données, et à quelles fins » (Comité des droits de l'homme. 1988)

Toutefois, l'Assemblée générale de l'ONU a adopté une résolution le 14 décembre 1990 , qui fixe certains principes généraux en matière de fichiers personnels informatisés. Cette résolution adoptée par l'assemblée générale des Nations Unies, a interdit la collecte et le traitement des données à caractère personnel selon des moyens illicites, ou déloyaux. Elle garantit une protection minimale des droits de l'homme dans ce domaine, notamment concernant les données dites sensibles (Résolution 45/95 1990).

Il existe d'autres dispositions dans des textes distincts d'organes de l'ONU, tels que L'OCDE, organisation internationale à vocation économique, qui a émis en 1980 une recommandation comportant des lignes directrices, régissant la protection de la vie privée, et les flux transfrontaliers de données.

L'OMC qui s'occupe du commerce international a également pris position pour la protection de la vie privée des personnes ainsi que pour la protection du caractère confidentiel des dossiers (La protection international des données personnelles sur internet 2018)

Toutefois, aucune de ces dispositions ne sont obligatoires. Elles traduisent, cependant, un consensus international et servent de fondements pour l'élaboration des règles de protection de la vie privée au niveau mondial (Desgens 2018)

2–2–Au niveau de l''union européenne

Quand en parle de l'union européenne il faut tout d' abord citer la Convention européenne des droits de l'homme (CEDH)((Convention européenne des droits de l'homme. 1953) qui, à son article 8 , protège la vie privée et familiale, le domicile et la correspondance. La CEDH ne consacre pas expressément la protection des données, mais on a intégré celle-ci à l'art. 8 CEDH.

Puis y as une convention du Conseil de l'Europe qui a été adoptée, à Strasbourg, le 28 janvier 1981(appelée : Convention 108) qui protège l'individu, en obligeant les États parties à la Convention, à adopter certains principes minimaux, afin de garantir une protection dans leur législation, concernant la transmission de données à d'autres États parties à la Convention. Selon son article 1er : «Le but de la présente convention est de garantir sur le territoire de chaque partie, à toute personne physique, quelle que soit sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant.» (Convention pour la protection des personnes a l'égard du traitement automatisé des données a caractère personnelles. 1981)

Grâce à la convention de Strasbourg, les données

personnelles font l'objet d'une protection équivalente en Allemagne, Autriche, Danemark, Espagne, France, Irlande, Islande, Luxembourg, Norvège, Royaume-Uni, Suède.

Puis au sein de l'Union européenne, le Parlement européen et le Conseil ont adopté le 24 octobre 1995, une directive « relative à la protection des personnes physiques, à l›égard du traitement des données à caractère personnel, et à la libre circulation de ces données. » Cette directive a pour objet « une protection équivalente de haut niveau dans tous les Etats membres de la Communauté, afin d'éliminer les obstacles aux échanges des données nécessaires au fonctionnement du marché intérieur. » (La directive(UE) 95/46/CE sur protection des données à caractère personne . 1995). Elle est complétée par la directive du 15 décembre 1997, « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.» (Directive(UE) 97/66/CE du Parlement européen et du Conseil 1997)

En 2016, l'Union européenne a adopté le règlement général sur la protection des données, l'une de ses plus grandes réalisations de ces dernières années. Ce règlement est venu remplacer la directive sur la protection des données de 1995, adoptée alors que l'internet n'en était qu'à ses débuts.

Le règlement général sur la protection des données clarifie notamment les règles applicables aux entreprises, et renforce également les droits des citoyens, en leur octroyant un droit à l'oubli, un droit à la portabilité des données, et le droit à l'information sur les failles de sécurité. Ces droits n'avaient aucune présence dans la directive précédente. Le règlement révisé réaffirme enfin, le rôle de contrôle et de supervision des autorités nationales, comme la Commission nationale de l'informatique et des libertés (CNIL) en France.

Autre nouveauté mise en avant par le règlement : une plus forte coopération entre les autorités nationales. Pour cela, un comité européen de la protection des données (EDPB) est créé, composé de représentants des autorités de protection des données de tous les Etats membres. Il vient compléter l'action du contrôleur européen de la protection des données. L'EDPB s'assure que la loi sur la protection des données est bien appliquée par tous les Etats membres, et que les autorités de protection des données coopèrent efficacement (Braibant, Guy 1998)

Ce nouveau règlement donne enfin à l'Union européenne, les moyens pour lutter d'une façon efficace, contre les transgressions perpétrées par des entreprises multinationales. Il impose en effet des sanctions en cas de violation du règlement. Le RGPD s'applique de fait à toutes les organisations et les entreprises ayant un exercice au territoire de l'Union européenne, et ce même si leur siège principal se trouve en dehors de l'UE. Ce règlement général est désormais reconnu par le droit de l'Union européenne, il place en effet l'individu au cœur d'un système juridique, technique et éthique qui renforce sa maîtrise de l'utilisation faite de ses données en lui conférant de nouveaux droits et garanties. Il s'appliquera chaque fois qu'un résident de l'Union se trouvera affecté par un traitement de données, ce qui signifie, et c'est là un changement d'envergure, qu'il s'imposera aux entreprises de toute la planète, dès lors qu'ils offriront un produit, ou un service à un citoyen européen. (Miller 2017)

Le règlement général sur la protection des données vient abroger la directive du 24 octobre 1995, qui était jusqu'alors le socle européen en ce qui concerne la protection et d'utilisation des données personnelles. Cette directive de 1995 a permis également une certaine harmonisation des législations des pays membres de l'UE sur le sujet, mais cette harmonisation était critiquer d'imparfaite et partielle, et qu'elle créait une «insécurité juridique» (RGDP s.d.)

Le règlement d'avril 2016 entend donner une vision commune et homogène de la protection des données personnelles dans l'UE. Il renforce le droit des individus sur leurs données. Dans son premier considérant, celui-ci précise d'ailleurs que la protection des données personnelles est un droit fondamental. Ce droit est consacré à la fois par l'article 8 de la Charte des droits fondamentaux de l'UE, et par l'article 16 du Traité sur le fonctionnement de l'UE (TFUE), qui disposent que : «toute personne a droit à la protection des données à caractère personnel là concernant». Ce droit n'est cependant pas absolu, et doit être concilié avec d'autres droits, comme la liberté d'entreprise (Article 04 de la Loi n°18/07 2018)

3–Le cadre juridique de la protection des données personnelles sur le plan national

Afin d'être en adéquation avec les législations internationales en la matière, le législateur algérien est intervenu pour règlementer la protection des données personnelles , en encadrant ce volet délaissé fort bien longtemps, en prévoyant un arsenal juridique, à caractère préventif mais aussi répressif, à travers la promulgation de la loi n° 18-07 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel (Sophie Haddad 2018) .

Cette loi la situe dans un contexte international de renforcement légal de la protection des données personnelles, et moins d'un mois après l'entrée en application du règlement général pour la protection des données personnelles des citoyens de l'Union Européenne (RGPD). Cette nouvelle loi contient plusieurs dispositions protégeant les données personnelles, qui peuvent être clarifiées comme suit :

3–1–Les droits des concernés et les obligations des traiteurs

Afin d'assurer une protection maximale des données à caractère personnel, le législateur algérien est intervenu pour protéger un éventail de droits pour les personnes concernées par le traitement, tout en imposant à l'organisme qui traite les données un ensemble d'obligations à respecter.

3–1–1–Les droits des concernés par les traitements des données

L'un des objectifs de la loi, est d'octroyer davantage de contrôle et de visibilité aux personnes concernées. Elle fixe ainsi des procédures et des mécanismes permettant à la personne concernée, d'exercer ses droits qui sont définis de façon précise, pour une bonne maitrise des informations les concernant. Ainsi, le responsable du traitement doit veiller à ce que les personnes au sujet desquels il collecte, enregistre et utilise des données puissent exercer les droits suivants :

-Le droit à l'information

Ce droit vient du principe fondamental, qui est le principe de loyauté et de transparence de la collecte du traitement de données à caractère personnel. Le responsable du traitement doit collecter et traiter les données de manière loyale, c'est-à-dire de manière transparente pour les personnes concernées. Ainsi, la loyauté du traitement implique nécessairement une information claire, précise et compréhensible de la personne concernée, par le traitement de données (Article 04 de la Loi n°18/07 2018). Et pour cela la collecte de ces données doit s'accompagner d'une information claire et précise des personnes sur :

-L'identité du responsable du fichier.

-La finalité du fichier.

-Les destinataires des données.

-Leurs droits (droit d'accès, de rectification, et d'opposition).

-les éventuels transferts de données vers des pays étranger. (Article 36 de la Loi n° 18-07 2018)

-Le droit à l'opposition

Le droit à l'opposition comme son nom l'indique, permet à la personne concernée de s'opposer au traitement de ces donnes personnelles .Toute personne a le droit de s'opposer pour des motifs légitimes au traitement de ses données, sauf si celui-ci répond à une obligation légale (ex : fichiers des impôts), ou lorsque l'application de ce droit a été écartée par une disposition expresse de l'acte autorisant le traitement. (Article 34 de la Loi n° 18-07 s.d.)

Le droit d'accès

Toute personne a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle. Ils peuvent également prendre connaissance de l'intégralité des données la concernant et pour cela toute personne peut :

-Accéder à l'ensemble des informations la concernant,

-Connaître l'origine des informations la concernant,

-Accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision la concernant (par exemple, les éléments qui auraient servi pour ne pas vous accorder une promotion ou le score attribué par une banque et qui a conduit au rejet de votre demande de crédit),

-En obtenir la copie, (des frais n'excédant pas le coût de la reproduction peuvent être demandés)

-exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées. (Article 35 de la Loi n° 18-07 s.d.)

Droit de rectification

Dit aussi «droit à l'effacement» ou «droit à l'oubli» : la personne concernée a le droit d'obtenir de la personne responsable du traitement des données personnelles, une rectification des données la concernant si elles sont inexactes. De même, la personne concernée pourra obtenir un effacement de ses données personnelles par le responsable du traitement. Toute personne a le droit donc de faire rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent. Les modifications demandées doivent être traitées au plus court délai. (Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée. Dans un formulaire en ligne, il peut se matérialiser, par exemple, par une case à cocher non cochée par défaut s.d.)

3-1-2- Les obligations des traiteurs des données

L'organisme chargé du traitement des données à caractère

personnel, est responsable d'un ensemble d'obligations faisant également l'objet de garanties pour les personnes concernées par le traitement, qui peuvent être présentées comme suit :

-L'accord préalable de la personne

La Loi pose l'obligation de recueillir « l'accord préalable » de la personne concernée par le traitement des données, qui doit être exprès, avec un droit de rétractation ouvert à tout moment. (l'article 04 de la Loi n° 18-07 2018)

Le texte 07 prévoit six (06) exceptions aux termes desquelles l'accord préalable n'est pas requis, et notamment dans les cas où le traitement est nécessaire au respect d'une obligation légale, à la sauvegarde de la vie de la personne concernée, à l'exécution d'un contrat auquel la personne concernée est partie, à la sauvegarde d'intérêts vitaux, à l'exécution d'une mission d'intérêt public, et à la réalisation d'un intérêt légitime.

Le législateur n'a pas négligé la protection des données à caractère personnel de l'enfant, et a stipulé le consentement préalable de son représentant légal. Ce consentement ne peut être dépassé sans l'autorisation du juge si l'intérêt supérieur de l'enfant l'exige (L'article 45 de la Loi n° 18-07 2018)

-Le respect des procédures préalables au traitement

L'organisme responsable du traitement des données à caractère personnel doit suivre les procédures prévues par la loi, qui figurent principalement dans la déclaration et l'autorisation, que nous aborderons comme suit :

-La déclaration préalable

Afin de renforcer la protection des données à caractère personnel, la loi impose à la partie responsable du traitement de fournir une autorisation préalable, contenant un ensemble de données de base à l'Autorité nationale de protection des données à caractère personnel, en tant qu'obligation de faire le traitement dans les limites autorisées par la loi.

-L'autorisation

Dans le cas où le traitement à effectuer comporte des dangers manifestes pour le respect et la protection de la vie privée et des libertés et des droits fondamentaux des personnes, l'autorité nationale décide de le soumettre au régime d'autorisation préalable.

À cette fin, il est interdit de traiter des données sensibles, sauf pour des motifs d'intérêt public indispensable, pour garantir l'exercice des fonctions légales ou statutaires du responsable du traitement, ou lorsque la personne concernée a donné son consentement exprès, en cas d'une disposition légale qui le consacre ou avec l'autorisation de l'autorité nationale. Ou dans les cas citer à l'article 18/3

3–2–La création de l'autorité nationale de protection des données à caractère personnel

Aux fins d'une sécurisation maximale, il a été créé, auprès du Président de la République, une autorité administrative indépendante. Son siège est à Alger. Elle a comme mission de veiller à ce que le traitement des données soit mis en œuvre, conformément aux dispositions de la présente loi. Cette autorité a également vocation de s'assurer que l'utilisation des technologies de l'information et de la communication, ne comporte pas de menaces. Et ce, au regard des droits des personnes, des libertés publiques et de la vie privée.

Et pour garantir une efficacité au sein de cette autorité, le législateur a tenu qu'elle soit composée de personnes compétentes,y compris de juges, juristes, et des représentants des ministres suivants : ministre de la défense nationale ministre des affaires étrangères ministre chargé de l'intérieur ministre de la justice, garde des sceaux ministre chargé de la poste, des télécommunications, des technologies et du numérique ministre chargé de la santé ministre du travail, de l'emploi et de la sécurité sociale.

En cas de violation des dispositions de la présente loi, le responsable du traitement sera soumis par cette autorité à certaines sanctions administratives qui consistent principalement en:

-L'avertissement,

-La mise en demeure,

-Le retrait provisoire pour une durée qui ne peut dépasser une année, ou le retrait définitif du récépissé de déclaration ou de l'autorisation,

-L'amende.

Les décisions de l'autorité nationale sont susceptibles de recours devant le Conseil d'Etat, conformément à la législation en vigueur (L'article 46 de la Loi n° 18-07 2018).

3–3–L'aspect dissuasif de la loi 18/07

Outre les sanctions administratives infligées à l'autorité nationale, en cas de violation des dispositions de cette loi, le législateur algérien a renforcé la protection des données à caractère personnel par des sanctions dissuasives (La loi n° 07/18 2018), dans lesquels 20 articles de loi 18/07 prévu pour diverses pénalités pouvant être imposées aux contrevenants. Ces peines vont de six mois à cinq ans d'emprisonnement et de 60 000 Da à 1 000 .000 Da

d'amende selon la gravité de l'infraction commise qui est principalement liée à la nature des informations en cause. Les peines prévues donc dans la présente loi qualifient ces violations de délits.

De plus Les personnes qui violent les dispositions de la présente loi, peuvent encourir les peines complémentaires prévues par le code pénal. Et en cas de récidive, les peines prévues sont portées au double.

La personne morale qui commet les infractions prévues par la présente loi, est punie conformément aux règles édictées par le code pénal. (L'article 70 de la Loi n° 18/07 2018)

Conclusion

Cette étude a mis en évidence un aspect grave de la protection de la vie personnelle de chacun d'entre nous. Il s'agit de protéger les données personnelles qui sont devenues les informations de référence dans les transactions de l'administration électronique

Nous avons noté que l'attention portée à la protection de la vie privée a commencé au niveau international, mais elle s'est davantage développée au niveau régional, où l'Union européenne est devenue un exemple de premier plan en matière de protection des données à caractère personnel, amenant le législateur algérien à adopter la même approche. Dans ce contexte, cette étude nous a permis d'atteindre plusieurs résultats importants qui peuvent être inclus comme suit :

-L'étude comparative nous a montré que la définition des données à caractère personnel différait en termes de rédaction dans différentes législations, mais elles étaient toutes identiques en termes de contenu en donnant une définition similaire limitée à l›attribution aux seules personnes physiques et à la spécificité du processus de traitement permettant de les identifier directement ou indirectement.

*Grâce à la grande expérience française en matière de protection des données à caractère personnel, l'Union européenne a pu mettre en place un système juridique cohérent entre tous les États membres. Et Depuis l'adoption du règlement général sur la protection des données à personnelles, ces données ont été protégées de manière particulière par la reconnaissance d'un éventail de droits aux personnes impliquées dans le processus de traitement. Ceci est encore renforcé par la création de **la Commission nationale de l'informatique et des libertés qui joue un rôle de contrôle et de supervision.**

-Le législateur algérien a tardé en matière de protection des données personnelles par rapport à la législation internationale. Mais il a récemment rectifié la situation en adoptant la loi 18/07 afin de se conformer à la législation internationale, en suivant la même approche. Dans ce contexte, le législateur algérien a reconnu un ensemble de droits pour les personnes physiques impliquées dans le processus de traitement en même temps il a imposé des obligations à l'organe responsable du traitement en plaçant tout cela sous la surveillance et le contrôle de **l'autorité nationale de protection des données à caractère personnel** et sous l'imposition de sanctions dissuasives.

Enfin, on peut dire que malgré l'intérêt croissant des différentes législations pour la protection des données à caractère personnel, ces systèmes sont encore défaillants dans de nombreuses lacunes juridiques qui ont conduit à une absence d'harmonie dans la pratique. Pour cette raison il est fort nécessaire de conclure une convention internationale sur la protection des données à caractère personnel en tant que référence à toute législation nationale garantissant :

-Les mêmes droits doivent être reconnus aux personnes concernées par le traitement partout dans le monde.

-Les organismes responsables du traitement doivent assumer les mêmes obligations dans toutes les législations des pays du monde.

-Assurer la conception et le développement de systèmes d'information et de logiciels pour assurer la sécurité des données personnelles contre le piratage.

Aussi la protection des données personnelles n'est pas effective sur les réseaux sociaux, le législateur algérien doit chercher à combler les failles que présentent la loi relative à la protection des données personnelles.

Références

Livres

1. Desgens Guillaime, 2018, La protection des données personnelles, Lexis Nexis, Paris.
2. Faucheux Sma,2018, Politique relative à la protection des données, Alamou groupe Europe Limted.
3. Haddad Sophie, Anne Lee, 2018, Antoine Casanova, RGPD : Evolution des droits et nouveaux droits reconnues aux personnes concernées par un traitement de données à caractère personnel, édition Carler.
4. Miller Richard,2017, La vie privée à l'ère des Big Data (dangers et opportunités de la révolution numérique), Centre Jean Gol.
5. Sitbon Caroline, 2001, Les données personnelles : Quel protection sur internet, CONFERENCE Mercredi 4 Avril 2001 Salon Lexposia Carousel du Louvre.

Documents internationaux

1. La Convention de sauvegarde des droits de l'homme et libertés fondamentales, plus connue sous le nom de Convention européenne des droits de l'homme a été ouverte à la signature à Rome le 4 novembre 1950 et est entrée en vigueur en 1953. Adopté à Rome, 4.XI.1950, amendée par les protocoles n°11et 14, complétée par le protocole additionnel et les protocoles n°4,6,7,12,13,16
2. Le pacte international relatif aux droits civils et politiques (PIDCP) a été adopté à New York le 16 décembre 1966 par l'Assemblée générale des Nations unies dans sa résolution 2200 A (XXI..
3. Comité des droits de l'homme, Observation générale 16, (23e session, 1988), Récapitulation des observations générales ou des recommandations générales adoptées par les organes créés en vertu d'instruments internationaux relatifs aux droits de l'homme, U.N. Doc. HRI/GEN/1/Rev.1, 21 (1994), paragraphe 10.
٤. Résolution 45/95, Principes directeurs pour la réglementation des fichiers personnels,68 iéme, séance plénière 14 décembre 1990.
5. La directive(UE) 95/46/CE sur protection des données à caractère personne Publiée au Journal officiel de l'Union européenne du 23 novembre 1995.
6. Directive(UE) 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.
7. La protection international des données personnelles sur internet, Note juridique n°06, septembre 2008, La commission juridique de l'Isoc France, 2018

Lois et règlements

1. Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel. Journal officiel N°34 du 10 juin 2018.
2. Le règlement n° 2016/679 ,RGPD, ou encore **GDPR**, de l'anglais *General Data Protection Regulation*) est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Applicable depuis le 25 mai 2018.

Rapports

1. Georges Chatillon, Les données personnelles : enjeux juridiques et perspectives, Rapport de Georges Chatillon, Université de Paris-I, Panthéon-Sorbonne,2016.
2. Guy Braibant : Données personnelles et société de l'information, rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46, Paris, le 3 mars 1998, texte téléchargé.

Ouvrages électroniques

1. Convention pour la protection des personnes a l'égard du traitement automatisé des données a caractère personnelles,1981, Strasbourg, disponible sur le lien: https://rm.coe.int/1680078b39, consulter le 07 /02 /2019
2. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible au : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
3. Protection des données (RGPD) : ce qui change,2020, disponible au **:** https://www.touteleurope.eu/actualite/protection-des-donnees-rgpd-ce-qui-change.html
4. Meunier Sophie, RGDP/ Que Signifie la notion des données personnelles, 2018, disponible au : https://www.itgovernance.eu/blog/fr/rgpd-que-signifie-la-notion-de-donnees-personnelles.
5. La Déclaration universelle des droits de l'homme (DUDH) est adoptée par l'Assemblée générale des Nations unies le 10 décembre 1948 à Paris par la résolution 217 (III) A,2019 disponible sur le lien : https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/frn.pdf
٦. Règlement général sur la protection des données : de quoi s'agit-il **? ,** 2018, disponible sur le lien : https://www.vie-publique.fr/eclairage/19588-rgpd-reglement-general-sur-la-protection-des-donnees-de-quoi-sagit-il

حماية المعطيات ذات الطابع الشخصي : اطار قانوني في تطور

ملخص

إن التقدم التكنولوجي الذي انعكس على الإدارة الالكترونية في الحياة المعاصرة جعلها سلاح ذو حدين من جهة ساهمت في توفير الجهد الوقت والمال في علاقاتها مع المنتفعين منها لكنها من جهة أخرى تسببت في ظهور مخاطر تمس بشكل مباشر بالحياة الخاصة للأشخاص. الأمر الذي استدعى ضرورة وضع نظام قانوني لحماية المعطيات الشخصية على المستوى الدولي وكذلك على المستوى الداخلي. وفي هذا السياق لم يتأخر المشرع الجزائري في حماية هذا الجانب من الحياة الخاصة للإفراد من خلال القانون 17/08 ليكون في انسجام مع التشريعات الدولية.

الكلمات المفتاحية
المعطيات الشخصية
معالجة المعطيات الشخصية
المعني بالمعالجة
المسؤول عن المعالجة
التنظيم العام لحماية البيانات

Protection of Personal Data: An Evolving Legal Framework

Abstract

The technological advance that has been reflected in e-government in contemporary life has transformed it into a double-edged weapon, since it has contributed to saving effort, time, and money in its relations with those who benefit from it, but it has also caused the emergence of risks affecting directly the privacy of individuals, which has required the establishment of a legal system for the protection of personal data at both national and international levels. In this context, the Algerian legislator has been quick in reacting to protect this aspect of individuals' privacy through Law 17/08 in order to be in alignment with international legislation.

Keywords
Personal data
processing of personal data
data subject
data controller
general data protection regulation