الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

LIVRE BLANC
SUR LA POTECTION
DES DONNEES PERSONNELLES

www.inpdp.tn

inpdp@inpdp.tn

www.facebook.com/inpdp.tn

www.youtube.com/channel/ucewcesim0pszpm_xrpjxc

Octobre 2021

1، نهج محمد معلى، ميتوال فيل، 1002، تونس ص.ب. 525
الهاتف (+216) 71 799 853 - 71 799 711 الفاكس 71 799 823

1, Rue Mohamed Moalla, 1002, Tunis, Tunisie B.P. 525
Tél. (+216) 71 799 853 - 71 799 711 Fax 71 799 823

Projet d'appui aux instances indépendantes en Tunisie
Financé par l'Union européenne et le Conseil de l'Europe
Mis en œuvre par le Conseil de l'Europe
UNION EUROPÉENNE CONSEIL DE L'EUROPE

Sommaire

I. Introduction

L'Instance Nationale de Protection des Données à Caractère Personnel (l'Instance ou INPDP, ci-après) a décidé de rédiger un livre blanc sur son domaine d'intervention, la protection des données. La mission a été réalisée avec le soutien de l'Union Européenne.

Les livres blancs doivent généralement être réalisés par des experts extérieurs à l'espace sur lequel ils portent pour préserver l'objectivité nécessaire du constat et de l'évaluation loin des partis pris et surtout ne pas défendre nécessairement la manière de voir des intervenants nationaux. Dans ce cadre, Monsieur Jean-Marc VAN GYSEGHEM, expert belge de la protection a été chargé de réaliser ce document.

Le livre blanc est destiné aussi bien aux citoyens tunisiens qu'aux entreprises et les autorités et structures publiques tunisiennes, mais il est utile pour les partenaires étrangers et les potentiels investisseurs pour évaluer le niveau de la protection sur le plan national. Comme la pratique l'a démontré dans les expériences comparées, le recours au livre blanc par une structure, en l'espèce l'INPDP, est très utile pour communiquer sur son domaine d'intervention.

Le livre blanc est ainsi rédigé par un expert dans le domaine qui éclaire le lecteur sur les normes et les bonnes pratiques en matière de protection des données personnelles. Il s'attachera à présenter le cadre juridique international de la protection et par la suite se penchera sur la situation au niveau national pour l'évaluer et proposer des pistes d'action pour en améliorer la conformité aux normes.

Dans ses *Essais* qui datent du XVI^{e} siècle, Montaigne écrivait déjà qu'*« Il faut se réserver une arrière-boutique toute nôtre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude* ». Cette notion d'arrière-boutique représente de manière très pertinente celle de la vie privée qui consiste à préserver du regard des autres individus des éléments de sa personne. Il ne s'agit nullement de cachoterie mais bien de réel pouvoir laisser à l'individu de choisir ce qu'il désire partager avec ses semblables. Prôner le contraire serait l'instauration de la dictature, du totalitarisme et de la surveillance généralisée contraires à la mise en place de la démocratie et de la protection des droits des individus.

Si la notion de vie privée est ancienne, elle est revenue sur l'avant-scène au terme de la seconde guerre mondiale qui a été synonyme d'anéantissement de toute vie privée par la mise en place de régime de contrôle total des individus aboutissant à la persécution de ceux qui ne correspondaient pas aux critères mis en place par le régime.

En réaction à cette politique de contrôle et de destruction, les états se sont engagés à respecter un certain nombre de principes de base en matière de protection des droits fondamentaux de tout individus notamment dans la Déclaration universelle des droits de l'Homme de 1948. Ce texte universel sera suivi par d'autres qui ont, pour affinés, certains aspects mais surtout apportés un régime de contrôle du respect de la dignité de l'être humain à l'image de la Convention européenne des Droits de l'Homme de 1950.

Nous allons déterminer dans les développements qui suivent, d'une part, les concepts-clef mais également les divers textes internationaux en matière de protection des données.

Tout individu a droit à cette protection qui est fondamentale dans une société démocratique dès lors qu'il faut lui donner les moyens de s'épanouir en toute liberté, étant entendu que sa liberté s'arrête là où celle de l'autre commence.

La protection des données est considérée comme fondamentale pour le développement de l'individu dans une société démocratique et à la construction de son bien-être. Elle est au service de l'Homme.

L'on doit également relever que cette protection s'étend également à la vie professionnelle de l'individu qui mérite également d'être protégé sur son lieu de travail. Ainsi, la Cour européenne des droits de l'homme a, à maintes reprises, réaffirmée à travers l'article 8 de la Convention européenne des droits de l'homme que cette protection *"peut s'étendre à des activités professionnelles ou commerciales"*[1].

Si cette protection est souvent liée à la protection de la vie privée, son champ d'application est beaucoup plus vaste que cela. En effet, plusieurs droits fondamentaux sont concernés. Pensons à la liberté d'expression, à la liberté d'association ou celle de l'information.

De manière assez récente, la Charte des droits fondamentaux de l'Union européenne[2] a élevé la protection des données à caractère personnel au rang de droit fondamental *in se* même s'il garde cette particularité de rester lier à d'autres.

Par ailleurs, une telle protection permet également d'éviter les discriminations entre individus basées, entre autres, sur les croyances religieuses, les appartenances syndicales, le sexe, la race, les données relatives à la santé ou les orientations sexuelles.

Outre ces considérations basées sur les droits humains fondamentaux eux-mêmes, l'on doit constater une réelle explosion des technologies de la communication et de l'information pouvant porter atteinte à ce droit à la protection des données à caractère personnel. Ces technologies ne se limitent pas aux activités commerciales mais aussi publiques avec l'émergence du concept de gouvernement électronique (eGov). Le développement de ces technologies implique la prolifération de bases de données informatiques servant d'endroit de stockage et de traitement de nombreuses données à caractère personnel. Ensuite, l'interconnexion de ces bases de données peut dévier vers une traçabilité de l'individu dans ses diverses activités qu'elles soient privées ou professionnelles.

Nous constatons dès lors que les technologies de la communication et de l'information prennent de plus en plus d'importance dans les prises de décision concernant des individus. Nombre de décisions reposent ainsi sur des informations contenues dans ces bases de données. Il faut donc éviter de voir les avantages de l'utilisation des technologies de l'information et de la communication affaiblir la protection des données à caractère personnel.

---

[1] C.E.D.H., 28.01.2003 (affaire Peck / Royaume-Unis ; requête n° 44647/98) ; Voir aussi CEDH. 16 février 2000, Amann/Suisse, § 65 ; CEDH. 16 décembre 1992, Niemietz/Allemagne, § 29 ; CEDH 25 juin 1997, Halford/Royaume-Uni, § 42-46

[2] Voir article 8 de la Charte des droits fondamentaux de l'Union européenne, www.europarl.europa.eu/charter/pdf/text_fr.pdf.

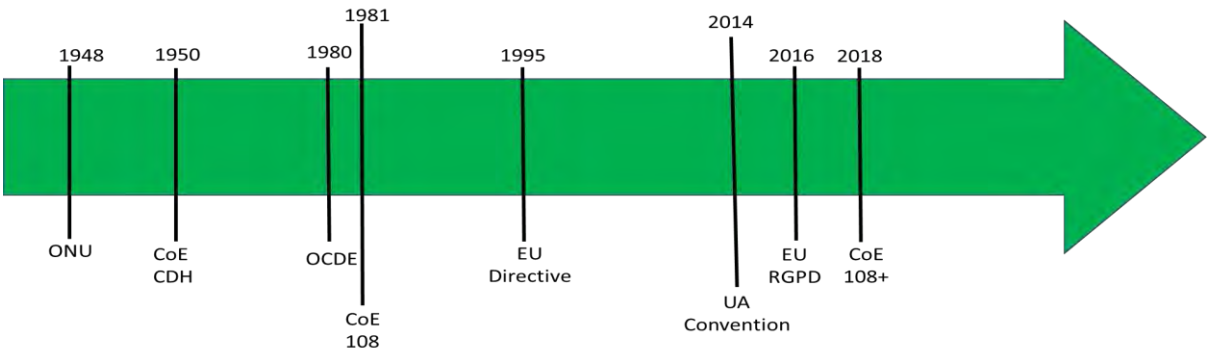
Cela implique que les informations doivent être correctes mais aussi pertinentes par rapport à l'objectif déterminé et déclaré du traitement. Il faut mettre en œuvre le principe selon lequel on ne peut collecter et traiter que les données à caractère personnel nécessaires à cette finalité. Par ailleurs, le responsable du traitement (c'est-à-dire la personne qui va déterminer la finalité/but du traitement et les moyens qui vont être mis en œuvre) a, une obligation de mise à jour des données et une limitation dans la collecte et le traitement. Par ailleurs, il doit veiller à ce que ces données ne soient pas divulguées sans autorisation de la personne concernée ou d'une disposition légale. Cela implique donc la mise en place de mesures organisationnelles et techniques assurant la sécurité du traitement impliquant, entre autres, la collecte et le stockage des données à caractère personnel.

Cette obligation de sécurité implique une responsabilisation du responsable du traitement (principe d'*accountability*) renforcée en fonction du type de données traitées. Il existe, en effet, des données qui sont moins sensibles que d'autres et qui demande une protection éventuellement moindre. Nous constatons, en effet, qu'il peut exister deux catégories de données qui peuvent être référencées. Il y a, d'une part, les données sensibles qui sont celles qui touchent l'individu dans ce qu'il a de plus précieux en termes de sphères privées et, d'autre part, les autres données. La première catégorie concerne des données à caractère personnel révélant, par exemple, l'appartenance religieuse, les origines ethniques, ou relatives à la santé. Cela peut également être les données génétiques qui ont cette particularité de concerner un grand nombre de personnes, étant celles d'une même fratrie.

Parallèlement à cela, il faut nécessairement donner à la personne concernée les moyens de contrôle sur le responsable via un droit d'accès duquel découlera, entre autres, un droit de rectification et d'opposition. Par ailleurs, on est dans l'obligation de mettre en place un régime de sanction afin de rendre la loi pleinement efficace. En effet, l'on constate qu'une loi sans sanction fait l'objet d'une désobéissance qui la rend parfaitement inefficace.

II. La protection des données à travers les normes internationales

L'analyse des textes internationaux révèle une histoire de la donnée à caractère personnel qui peut se résumer comme suit :



Pour une question de méthodologie, il a été décidé de présenter les différents textes non pas de manière chronologique mais en fonction de leur portée internationale en commençant par l'ONU.

A. Organisation des Nations Unies (ONU)

Il faut garder à l'esprit que : *"L'Organisation internationale des Nations Unies a été fondée en 1945, après la Seconde Guerre mondiale, par 51 pays déterminés à maintenir la paix et la sécurité internationales, à développer des relations amicales entre les nations, à promouvoir le progrès social, à instaurer de meilleures conditions de vie et à accroître le respect des droits de l'homme."*

L'objectif de l'ONU est donc d'assurer la paix internationale mais aussi de développer des instruments pouvant garantir le respect des droits de l'homme ; contexte dans lequel la Déclaration universelle des droits de l'homme a été adoptée par les 58 pays membres en 1948.

Par la suite, l'ONU a adopté de nombreux documents en ce sens dont les "Principes directeurs pour la règlementation des fichiers personnels informatisé" en décembre 1990 (résolution 45/95 de l'Assemblée générale) qui mettent en place les principes suivants :

1. Principes de détermination des finalités et de nécessité/pertinence

Le texte appuie sur le fait que le traitement doit poursuivre une finalité préalablement déterminée et légitime. De manière conséquente à cette obligation, les données traitées doivent être adéquates et mises à jour mais également ne pas pouvoir être traitées pour une autre finalité qui serait considérée comme incompatible sans autorisation de la personne concernée, etc.

De plus, en imposant un critère de pertinence des données, le texte insère la notion de nécessité des données au regard de la finalité poursuivie.

2. SÉCURITÉ

L'ONU impose que des mesures de sécurité soient prises pour protéger les dossiers contre des dangers naturels (perte accidentelle) et des dangers humains (accès non autorisés, etc.).

3. FLUX TRANSFRONTIÈRE

Le transfert de données vers un état ne peut être effectué que si la législation dudit état offre des garanties similaires.

B. ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUE (OCDE)

L'OCDE a été créée en 1961 et promeut *"les politiques qui amélioreront le bien-être économique et social partout dans le monde"*[3].

"L'OCDE offre aux gouvernements un forum où ils peuvent conjuguer leurs efforts, partager leurs expériences et chercher des solutions à des problèmes communs. Nous travaillons avec les gouvernements afin de comprendre quel est le moteur du changement économique, social et environnemental. Nous mesurons la productivité et les flux mondiaux d'échanges et d'investissement. Nous analysons et comparons les données afin de prédire les tendances à venir. Nous établissons des normes internationales dans un grand nombre de domaines, de l'agriculture à la fiscalité en passant par la sécurité des produits chimiques."[4]

Dans cette optique, l'organisation a adopté des recommandations relatives à la protection de la vie privée et, plus particulièrement, des données à caractère personnel.

1. "LES LIGNES DIRECTRICES RÉGISSANT LA PROTECTION DE LA VIE PRIVÉE ET LES FLUX TRANSFRONTIÈRES DE DONNÉES"

En 1980, l'OCDE a adopté *« Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données »* sous forme de recommandation ; document qui a été amendé en 2013[5].

Ce texte, assez précurseur dès lors qu'il est antérieur à toute autre réglementation internationale en la matière, repose sur les trois piliers de l'OCDE, *« à savoir : la démocratie pluraliste, le respect des droits de la personne humaine et l'économie de marché ouverte »*.

En guise de préface, le document énonce que :

> *« Les Lignes directrices sur la vie privée représentent un consensus international sur des orientations générales concernant le recueil et la gestion d'informations de caractère personnel. Les principes énoncés dans ces Lignes directrices se caractérisent par leur clarté et leur souplesse d'application et par leur formulation, qui est suffisamment générale pour leur permettre de s'adapter au changement technologique. Les principes couvrent l'ensemble des supports pour*

[3] http://www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html
[4] http://www.oecd.org/pages/0,3417,fr_36734052_36734103_1_1_1_1_1,00.html
[5] https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188

le traitement informatisé de données relatives aux personnes (depuis les ordinateurs locaux jusqu'aux réseaux aux complexes ramifications nationales et internationales), tous les types de traitement de données de caractère personnel (depuis l'administration du personnel jusqu'à la compilation de profils de consommateurs) et toutes les catégories de données (depuis les données de trafic jusqu'aux données sur les contenus, et des plus banales aux plus sensibles). Les principes sont applicables aux échelons tant national qu'international. Au fil des ans, ils ont été repris dans un grand nombre d'instruments nationaux, s'appuyant aussi bien sur la réglementation que sur l'autorégulation, et ils sont toujours largement utilisés dans les secteurs tant public que privé. »

Ces lignes directrices, qui s'appliquent tant au domaine privé qu'au domaine public sans distinction, se veulent technologiquement neutres. Cela signifie qu'elles ne veulent pas viser une technologie au détriment d'une autre, compte-tenu de leur évolution rapide.

En outre, elles posent les principes fondateurs de la protection des données à caractère personnel.[6]

L'OCDE met en place des principes en ayant préalablement définit 3 termes que sont le "Maître de fichier", les "données à caractère personnel" et le "flux transfrontière de données à caractère personnel" :

- Par Maître de fichier, le texte entend la *« personne physique ou morale qui est habilité à décider du choix et de l'utilisation des données à caractère personnel. »*.
- Les Données à caractère personnel sont définies, quant à elle, comme *« toute information relative à une personne physique identifié ou identifiable »* qui est la personne concernée.
- L'OCDE définit également la notion de flux transfrontière qui concerne la circulation de données à caractère personnel entre pays.

L'OCDE, à l'instar de l'ONU, considère comme fondamental que les finalités pour lesquelles les données sont traitées soient déterminées au plus tard au moment de la collecte et que le traitement ne pourra avoir lieu que dans le cadre de ces finalités à l'exclusion de toute autre sauf exception de compatibilité. Cette exception consiste en la possibilité de poursuivre une autre finalité qui ne soit pas incompatible avec la ou les premières. Pour savoir si une finalité est compatible ou pas, on utilisera – entre autres – le critère de la conscience par la personne à laquelle les données sont liées qu'une telle finalité pouvait être poursuivie.

Le principe de nécessité qui constitue une des pierres angulaires de toute législation relative à la protection des données à caractère personnel est également prôné par l'OCDE qui précise que seules les données nécessaires à la finalité du traitement pourront être collectées et traitées. Cela implique également le concept de pertinence qui est directement lié à la finalité du traitement.

[6] En effet, il aurait été moins ambigu de parler de lignes directrices régissant la protection des données à caractère personnel. En effet, la protection des données à caractère personnel touche plusieurs droits fondamentaux et pas uniquement la vie privée.

Un corollaire à ce principe de nécessité, les données traitées doivent être exactes, ce qui implique qu'elles doivent être complètes et mises à jour. En outre, elles ne peuvent, par ailleurs, pas être conservées au-delà du temps nécessaire pour atteindre la finalité.

Nous devons relever que l'OCDE n'a pas souhaité opérer une différence entre les différents types de données (sensible ou pas) au motif que cette classification dépendait d'un pays et d'une culture à l'autre.

Comme contrepartie à la possibilité de traiter des données à caractère personnel, le Maître de fichier doit assurer une sécurité capable de protéger le traitement de toute détérioration, destruction ou accès/utilisation non autorisé.

L'OCDE érige également en principe la transparence du traitement (finalités, type de données, etc) de manière telle que la personne concernée en soit informée et qu'elle puisse exercer ses droits.

Une obligation de responsabilité sur le respect des lignes de conduites repose sur les épaules du maître de fichier, à l'instar de bon nombre d'autres législations.

Dans le cadre de cet *accountability*, le texte énonce également l'existence d'une autorité de contrôle.

2. DÉCLARATION SUR LES FLUX TRANSFRONTIÈRES DE DONNÉES[7]

Le 11 avril 1985, l'OCDE a adopté une Déclaration sur les Flux transfrontières de données suite à la constatation que les technologies se développent extrêmement vite et que la conséquence en est une augmentation des flux de données à caractère personnel, et plus particulièrement au niveau des états membres. L'objectif est, à l'instar des lignes directrices vues ci-dessus, économique. Cela se concrétise par une déclaration d'intentions de la part des Etats membres.

3. DÉCLARATION RELATIVE À LA PROTECTION DE LA VIE PRIVÉE SUR LES RÉSEAUX

L'OCDE a présenté, en 1998, une déclaration par laquelle les états membres réaffirment *« leur engagement à l'égard de la protection de la vie privée sur les réseaux mondiaux, afin d'assurer le respect de droits importants, de construire la confiance dans les réseaux mondiaux et d'empêcher des restrictions inutiles aux flux transfrontières de données de caractère personnel »* et qu'*« ils s'attacheront à établir des passerelles entre les différentes approches adoptées par les pays Membres en vue de garantir la protection de la vie privée sur les réseaux mondiaux sur la base des Lignes directrices de l'OCDE »*.

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

4. RECOMMANDATION DE L'OCDE RELATIVE À LA COOPÉRATION TRANSFRONTIÈRE DANS L'APPLICATION DES LÉGISLATIONS PROTÉGEANT LA VIE PRIVÉE

En 2007, l'OCDE a adopté une recommandation mettant en valeur la coopération transfrontière partant de la constatation que :

> *"La mondialisation, l'émergence de modèles économiques de «suivi du soleil», l'essor de l'Internet et l'effondrement des coûts des télécommunications augmentent considérablement le volume des informations de caractère*

[7] www.oecd.org/fr/sti/hautdebit/declarationdelocdesurlesfluxtransfrontieresdedonnees.htm

personnel qui franchissent les frontières. Cet accroissement de la circulation transfrontière de l'information a des retombées positives tant pour les organisations que pour les personnes en abaissant les coûts, en induisant des gains d'efficience et en améliorant le service au client. Dans le même temps, ces flux d'informations de caractère personnel accentuent les préoccupations pour la vie privée, en soulevant de nouveaux problèmes de protection des informations de caractère personnel des individus."

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

Ce document a aussi prévu l'établissement d'une autorité de contrôle.

C. CONSEIL DE L'EUROPE

Le Conseil de l'Europe a été créé en 1949 et comptait en son sein 10 pays fondateurs. A l'heure actuelle, 47 pays sont membres. L'assise territoriale du Conseil de l'Europe est le continent européen. En d'autres termes, seuls les pays ayant une partie de ou tout leur territoire sur la plaque continentale européenne peuvent devenir membre du Conseil de l'Europe.

> *"Le but premier du Conseil de l'Europe est de créer sur tout le continent européen un espace démocratique et juridique commun, en veillant au respect de valeurs fondamentales : les droits de l'homme, la démocratie et la prééminence du droit."*[8]

Un des objectifs est de *"défendre les droits de l'homme, la démocratie pluraliste et la prééminence du droit"*[9].

1. CONVENTION DE SAUVEGARDE DES DROITS DE L'HOMME ET DES LIBERTÉS FONDAMENTALES

Convention de sauvegarde des droits de l'homme et des libertés fondamentales a été signée en 1950 à Rome et amendée à plusieurs reprises. Elle reprend les droits fondamentaux de l'Homme.

L'article qui concerne la protection de la vie privée est l'article 8 qui est libellé comme suit :

> *"1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
>
> *2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et*

[8] http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=fr
[9] http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=fr

à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui."

Il y a donc un régime de protection relativisé par une exception d'ingérence de la part des Etats ; ingérence qui est assortie de conditions. En effet, il faut que :

- L'ingérence soit prévue par une loi, ce qui signifie qu'il y a une obligation de transparence pour permettre aux citoyens de pouvoir déterminer les conditions dans lesquelles s'applique cette ingérence et contrôler sa légalité.
- Il faut que cette ingérence soit nécessaire dans une société démocratique, ce qui signifie qu'il faudra toujours analyser la situation pour voir si une mesure moins attentatoire à la vie privée est possible.
- Il faut que cette ingérence s'inscrive dans des domaines bien précis prévu par l'article 8 lui-même.

La Convention crée également la Cour européenne des droits de l'homme (CEDH) qui sert d'autorité de contrôle de la bonne exécution de la Convention par les états signataires et peut être saisie par tout bénéficiaire de la convention en cas de violation par un Etat signataire.

La jurisprudence de cette Cour est un précieux instrument en matière de droits fondamentaux dont la protection de la vie privée et des données à caractère personnel en particulier.

Nous pouvons citer quelques arrêts importants tels que :

- CEDH, arrêt Rekvényi c. Hongrie du 20.05.1999 ;
- CEDH, Evans c. Royaume-Uni, no 6339/05, 2007-
- CEDH, Marper c. Royaume-Uni, requêtes nos 30562/04 et 30566/04, 04.12.2008,
- CEDH, Güzel *Erdagöz c. Turquie*, requête n° 37483/02, 21.10.2008,
- CEDH, Odièvre c. France, requête no 42326/98 ;
- CEDH, Mikulić c. Croat*ie*, requête n° 53176/99.

2. CONVENTION 108 - 108+ POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

La convention 108 a été signée en 1981 et a servi de base à de nombreuses législations européennes par la suite. Il en a été ainsi pour la Directive européenne 95/46 et les législations nationales qui en découlent. Cette convention a également été rédigée en collaboration avec l'OCDE.

Le terme "convention" a été préféré à celui de "convention européenne" pour permettre à des pays non membres du Conseil de l'Europe de l'adopter[10]. Il est important de relever que la Tunisie y a adhérée en 2017[11].

Cela est explicitement prévu à l'article 23 de la Convention qui prévoit que :

[10] Voir le rapport explicatif de la convention, §24.
[11] www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=SfZxxakC

« 1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra inviter tout Etat non membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au comité.

2 Pour tout Etat adhérant, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe. »

Il est utile de relever que la convention fait l'objet d'une révision en vertu de l'article 19 qui prévoit que le Comité consultatif constitué après l'entrée en vigueur de la Convention.

"Le comité consultatif :

a. peut faire des propositions en vue de faciliter ou d'améliorer l'application de la Convention ;

b. peut faire des propositions d'amendement à la présente Convention conformément à l'article 21 ;

c . formule un avis sur toute proposition d'amendement à la présente Convention qui lui est soumis conformément à l'article 21, paragraphe 3 ;

d. peut, à la demande d'une Partie, exprimer un avis sur toute question relative à l'application de la présente Convention."

L'objectif de cette convention est clairement *"la protection juridique des individus vis-à-vis du traitement automatisé des données à caractère personnel les concernant"*. L'on se place ainsi au niveau des individus et non plus à celui des états avec leurs intérêts économiques. Cela est dans la logique-même du travail du Conseil de l'Europe qui a été créé avec, comme un des objectifs, de *"défendre les droits de l'homme, la démocratie pluraliste et la prééminence du droit"*[12]

Le centre de gravité est donc déplacé d'une dimension économique vers une dimension droits humains fondamentaux. Nonobstant ce déplacement, nous retrouvons des principes fondamentaux à ceux des Lignes directrices de l'OCDE.

En 2018, une convention 108 modernisée a été adoptée et surtout adaptée aux évolutions importantes en la matière par rapport à 1981. Certains termes et notions se sont ainsi vues modifiées. Dans le cadre du présent Livre blanc, nous allons retenir la Convention 108 modernisée (Convention 108+).

Au niveau des définitions, nous retrouvons des notions très similaires, si pas identiques, à celles données par l'OCDE. Ainsi, la convention contient cinq définitions de termes/notion importantes en la matière, à savoir « données à caractère personnel», «traitement de données», «responsable du traitement», « destinataire » et « sous-traitant».

A l'instar de l'OCDE, la convention prévoit que les finalités du traitement doivent être déterminées et légitime. Cela implique donc qu'aucun traitement ne pourra être effectué pour une autre finalité que celle qui a été déterminée préalablement à la collecte. Un

[12] http://www.coe.int/aboutcoe/index.asp?page=nosObjectifs&l=fr

critère de proportionnalité est également introduit dès lors que *« le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu »*[13].

La convention prévoit également que seules les données nécessaires à atteindre la finalité seront traitées ou de manière compatible avec cette première finalité. Cela introduit donc le concept de traitement ultérieur compatible avec la première finalité. Le critère de détermination de la compatibilité est équivalent à celle énoncée dans la cadre de l'OCDE, c'est-à-dire que l'on utilisera – entre autres – le critère de la conscience par la personne à laquelle les données sont liées qu'une telle finalité nouvelle pouvait être poursuivie.

Par ailleurs, les données traitées doivent être exactes et mises à jour. La convention stipule également que les données à caractère personnel devront être effacées ou rendues anonymes aussitôt qu'elles ne sont plus nécessaires à la finalité. Il faut relever que certaines données telles que celles relatives à la santé, à l'origine raciale ne peuvent être traitées *«qu'à la condition que des garanties appropriées, venant compléter celles de la [Convention 108+], soient prévues par la loi [nationale] »*[14]. Les états membres devront donc prévoir des garanties appropriées à ces données qualifiées de particulièrement sensibles.

Les données à caractère personnel doivent faire l'objet de *« mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation »*[15].

Au niveau de la transparence, le responsable du traitement doit informer la personne concernée avec un certain nombre d'éléments, dont ses droits pouvant être exercés auprès de ce responsable du traitement tels que les droits d'accès, de rectification, d'effacement et de recours. Cela permettra également à la personne de donner, le cas échéant, un consentement éclairé si cela est requis.

La Convention 108+ favorise les flux transfrontières des données à caractère personnel et prévoit les autorités de contrôle.

D. L'UNION EUROPEENNE

L'union européenne a été portée sur les fonts baptismaux en 1957 sous la dénomination de la Communauté économique européenne ou marché commun. Actuellement, l'Union européenne (UE) forme un partenariat politique et économique entre 28 pays européens (à partir du 1er février 2020, probablement 27).

Il y a, par ailleurs, une dimension "humaine" dès lors que l'Union européenne a mis en place des mesures de protection des droits humains.

L'Union européenne a, en 2010, mis en place diverses initiatives dont celle que l'on appelle "la stratégie numérique pour l'Europe" ("digital agenda" en anglais):

[13] Voir article 5.1 de la Convention 108+.
[14] Article 6 de la Convention 108+.
[15] Article 7 de la Convention 108+.

"Cette stratégie a pour but de tracer une voie afin d'exploiter au mieux le potentiel social et économique des TIC, surtout de l'internet qui constitue désormais le support essentiel de toute activité économique et sociétale, qu'il s'agisse de faire des affaires, de travailler, de s'amuser, de communiquer ou de s'exprimer librement. Mise en œuvre avec succès, cette stratégie sera un facteur d'innovation, de croissance économique et de progrès dans la vie quotidienne des particuliers comme des entreprises. Le déploiement plus large et l'utilisation plus efficace des technologies numériques permettront donc à l'Europe de relever les principaux défis auxquels elle est confrontée et procureront aux Européens une plus grande qualité de vie sous la forme, par exemple, de meilleurs soins de santé, de solutions de transport plus sûres et plus efficaces, d'un environnement plus propre, de nouvelles possibilités de communication et d'un accès plus aisé aux services publics et au contenu culturel."[16]

Certaines dispositions de cette stratégie touchent de près ou de loin la protection des données à caractère personnel.

1. LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

En 1995, l'UE a adopté la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; directive adoptée sur la base des compétences de l'Union européenne, c'est-à-dire sur un socle économique : la libre circulation des biens, des services et des personnes. Il est utile de tenir cela à l'esprit car le but premier de ce texte est de garantir une protection équivalente dans tous les Etats membres pour permettre cette libre circulation.

Cette directive a cependant été remplacée, en mai 2016 avec entrée en vigueur en mai 2018, par le Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD)

Nous retrouvons, dans la directive, les mêmes principes que ceux présents dans les textes déjà analysés (OCDE, Conseil de l'Europe) et nous proposons de ne pas les revoir dans cette section-ci.

L'on doit noter que la Cour de Justice de l'Union européenne (CJEU) a rendu des arrêts mettant en balance les principes de la directive 95/46/RGPD avec ceux d'autres directives :

- CJEU, C-28/08 P, Commission c/ Bavarian Lager, arrêt du 29.06.2010 ;
- CJEU, C-92/09 et 93/09, Volker und Markus Schecke GbR et Hartmut Eifert / Land Hessen, arrêt du 09.11.2010.
- CJUE, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, 5 juin 2018

16 http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-fr.pdf.

- CJUE, Tietosuojavaltuutettu c. Jehovan todistajat – uskonnollinen yhdyskunta, 10 juillet 2018

Si certaines définitions sont très semblables à celles figurant dans les précédents actes analysés, le RGPD en rajoute un grand nombre ou en modifie la portée.

Ainsi, l'on parle de responsable du traitement qui est un terme modifiant la portée par rapport à la notion de maître de fichier. La modification n'est pas uniquement de terminologie mais la portée est différente. En effet, les responsabilités de ce responsable de traitement portent sur tout le traitement.

Le RGPD définit le sous-traitant comme étant la personne avec laquelle le responsable du traitement contracte pour qu'elle effectue une partie du traitement pour son compte.

Un traitement est défini comme *"toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés appliqués à des données à caractère personnel …"*[17]. Il est important de relever que le procédé utilisé ne doit pas être spécifiquement automatisé. Cela implique qu'un traitement manuel de données à caractère personnel pourra entrer dans le champ d'application de la directive à condition que les données soient intégrées dans un fichier défini par cette directive.

Le RGPD reprend les concepts d'accountability, licéité, qualité de données, droits de la personne concernée, etc.

Au niveau des flux de données vers un pays tiers (pays hors de l'UE et de l'EEA), un certain nombre de processus sont mis en place dont le plus intéressant mais aussi le plus contraignant qui est la décision d'adéquation. Cette décision est le terme d'un processus durant lequel la Commission européenne analyse le régime de protection des données dans le pays tiers demandeur afin de vérifier s'il offre une protection adéquate. Si tel est le cas, une décision d'adéquation pourra être prise. Cela aura pour effet de permettre le transfert de données entre l'Union européenne et le pays tiers en assimilant ce dernier à un pays membre de l'Union européenne d'un point de vue de protection des données. Cette adéquation fait l'objet d'une vérification au moins tous les 4 ans par la Commission européenne.

Le régime de sanction a été fortement renforcé au niveau, d'une part, des compétences des autorités de contrôle et, d'autre part, des montants qui peuvent atteindre 20 millions d'Euro ou, s'il s'agit d'une entreprise, 4% du chiffre d'affaire mondial.

Le RGPD introduit également des droits nouveaux tels que le droit à la portabilité qui permet à la personne concernée *« de recevoir les données à caractère personnel [la] concernant qu' [elle a] fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et [a] le droit de transmettre ces données à un autre responsable du traitement »*[18].

2. RÉSOLUTION DE MADRID

La Résolution de Madrid est un instrument non contraignant adopté en novembre 2009 à Madrid de manière internationale. Cela signifie que cette résolution est un document qui

[17] Article 4 du RGPD.
[18] Article 20.1 du RGPD.

peut servir à l'adoption ou la modification de régimes de protection des données à caractère personnel par les Etats signataires sans qu'ils n'y soient obligés.

L'objectif premier de ce texte est de faciliter les flux transfrontières, point qui soulèvent des questions de protection des données à caractère personnel différente dans les pays. Comment doit procéder un responsable de traitement qui souhaite transférer des données à caractère personnel vers un partenaire situé à l'étranger. Comment peut-il s'assurer que le régime de protection en vigueur dans ce pays tiers assure une bonne protection ?

Ce texte souhaite donc faciliter ces transferts en proposant des règles "universelles" de protection des données à caractère personnel afin de faciliter ces flux.

Il introduit également, à l'article 11, le concept d'"accountability" qui impose au *responsable "qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent".* Cela signifie que le responsable a la charge de s'assurer que les dispositions de protection des données à caractère personnel sont respectées et qu'il s'assure qu'il a pris les mesures nécessaires pour y parvenir.

E. CONVENTION DE L'UNION AFRICAINE

L'Union africaine a adopté à Malabo (Guinée équatoriale) le 27 juin 2014 une convention relative à la cybersécurité et protection des données et à la cybercriminalité. Elle n'entrera en vigueur qu'après la quinzième ratification. A la date de juin 2020, seuls 14 signatures et 8 ratifications ont été enregistrés. La Tunisie fait partie depuis 2019 des Etats signataires mais pas encore membre.

Cette convention régionale reprend les dispositions que l'on retrouve dans les conventions du Conseil de l'Europe de Strasbourg sur la protection des données personnelles et celle de Budapest sur la cybercriminalité. Mais l'Afrique se caractérise par la décision de vouloir joindre ces deux domaines dans un même texte conventionnel ce qui explique peut-être le retard de son entrée en vigueur.

III. Les principes clefs de la protection des données personnelles

La protection des données à caractère personnel a donné lieu à l'émergence de principes clefs qui vont de pair avec l'étendue que l'on veut donner à une telle protection.

L'on retrouve cela dans le champ d'application de la directive qui prévoit que les traitements *"effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques"*[19] n'y entre cependant pas.

A. DEFINITIONS

Les définitions sont fondamentales pour une bonne compréhension des termes utilisés mais aussi permettent d'effectuer des liens entre législations tant internationales que nationales.

Si toutes les législations traitant de la protection des données n'ont pas les mêmes définitions, il n'en demeure pas moins que les notions sont similaires.

Par ailleurs, il faut également observer que des termes ont été modifiés avec le temps et suite à une meilleure appréciation des concepts. Il en va ainsi, à titre d'exemple, de Maître de fichier qui est devenu "responsable du traitement".

1. DONNÉES À CARACTÈRE PERSONNEL

Nous attirons l'attention sur le fait que cette notion ne devrait viser qu'une personne physique à l'exclusion des personnes morales. Cette limitation peut s'expliquer par le fait que l'on traite d'un droit fondamental qui, par définition, n'est l'attribut que des dites personnes physiques.

Par ailleurs, la notion est extrêmement large dès lors qu'elle vise toute information sans aucune limitation mais il faut que cette information soit liée à une personne identifiée ou identifiable. Si le premier terme est assez évident à comprendre tel n'est pas le cas du second qui donne lieu à beaucoup de discussion. Pour en comprendre la portée, nous pouvons nous reporter au considérant 26 du RGPD qui précise que *"pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci."*. Pour considérer qu'une personne soit identifiable, le responsable de traitement devra donc vérifier si lui-même ou toute autre personne peut identifier la personne. Cela rend, bien évidemment, également la définition extrêmement large dès

[19] Article 3.2.

lors que, dès l'instant où quelqu'un pourra identifier la personne concernée, il s'agira d'une donnée à caractère personnel.

Ces données à caractère personnel peuvent être le nom, le prénom, les adresses IP, un *log*, etc. Des images vidéos doivent également être considérées comme des données à caractère personnel ainsi qu'un test d'haleine pour autant que l'identification de la personne physique y liée ne requiert pas des moyens déraisonnables.

Il est utile d'analyser cette notion de manière contextuelle et en rapport avec la finalité du traitement. Ainsi, une prise de sang pourrait être considérée comme ne contenant pas de données à caractère personnel dans le chef du citoyen lambda au contraire des forces de police qui ont les moyens techniques pour procéder à son analyse.

L'information peut être liée tant à la sphère privée que publique. La Cour européenne des Droits de l'Homme du Conseil de l'Europe a ainsi précisé dans son arrêt Nimietz c. Allemagne du 16.12.1992 que :

> *"Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission, le confirme : dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort. Spécialement, les tâches d'un membre d'une profession libérale peuvent constituer un élément de sa vie à un si haut degré que l'on ne saurait dire en quelle qualité il agit à un moment donné."*[20]

2. RESPONSABLE DU TRAITEMENT

Les autorités européennes de protection de données à caractère personnel ont considéré qu'*"être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres"*[21]. Il s'agira bien souvent d'une analyse factuelle, qui oblige, par exemple, à vérifier si le responsable du traitement peut être considéré comme tel. *Il est établi que « la détermination des finalités et des moyens revient à établir respectivement le «pourquoi» et le «comment» de certaines activités de traitement. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le «pourquoi» et le «comment» pour être qualifiée de responsable du traitement. »*[22] et que *« lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable du traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant. Ces définitions prennent tout leur sens lorsque divers acteurs interviennent dans le traitement de données à caractère personnel et qu'il est nécessaire de déterminer lesquels d'entre eux sont responsables du traitement (seuls*

[20] C.E.D.H., Nimietz c. Allemagne, 16.12.1992, § 29.
[21] Groupe de l'article 29, *Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant»*, WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.
[22] Groupe de l'article 29, Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.

ou conjointement avec d'autres) et lesquels sont à considérer comme des sous-traitants, le cas échéant."[23]

Par finalité, l'on entend l'objectif poursuivi par le responsable de traitement, le "pourquoi" ci-dessus tandis que les moyens, pour leur part, expriment la façon par laquelle on atteindra l'objectif, la finalité et pourront être techniques mais aussi organisationnelles.

3. SOUS-TRAITANT

Pour être considéré comme sous-traitant, l'on ne peut pas être dans une relation hiérarchique avec le responsable de traitement et l'on doit traiter des données à caractère personnel pour son compte. Bien souvent, le sous-traitant interviendra sur les moyens mis en œuvre pour atteindre les finalités dès lors qu'il sera fait appel à lui pour ses compétences particulières. Ce sera le cas de fournisseurs de service Internet ainsi que les fournisseurs de *cloud computing*[24].

Il important de relever que dès l'instant où le sous-traitant est impliqué dans la détermination des finalités ou moyen, il sera considéré comme responsable du traitement conjoint.

4. TRAITEMENT

Le traitement est un ensemble d'opération extrêmement large et va de la collecte jusqu'à la destruction de la donnée en passant par tous les stades de « manipulation » de la donnée.

Il est également utile de relever que la notion de traitement ne doit pas s'appliquer uniquement lors d'opérations à l'aide de procédés automatisés mais également à des traitements manuels au cours duquel les données sont ordonnées en fonction de critères déterminés de manière telle qu'elles sont aisément accessibles.

B. DETERMINATION DES FINALITES

Ce principe essentiel est omniprésent dans les divers textes internationaux analysés. La détermination des finalités est un aspect du principe de transparence et doit permettre à la personne dont on traite les données (personne concernée) de pouvoir appréhender tout traitement auquel ses données à caractère personnel sont soumises.

La finalité doit être précise dans un double objectif :

- permettre à la personne concernée d'effectuer un contrôle et d'exercer, le cas échéant, les droits qui lui sont conférés par la législation.
- permettre au responsable de traitement de déterminer les données qui devront être collectées et traitées.

[23] Groupe de l'article 29, Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.
[24] Voir à ce propos, J. – M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel : mise en ménage possible ?", *R.D.T.I.*, issue 42, pp. 35-50. Voir également Groupe de l'article 29, "Avis 05/2012 sur l'informatique en nuage", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

Il s'agit donc d'une étape essentielle en matière de protection des données à caractère personnel.

La finalité doit également être explicite, ce qui signifie qu'elle doit être annoncée, ne pas être tenue *"secrète"* ou *"camouflée"*[25]

Il est également utile de rappeler que la finalité doit être légitime, ce qui signifie que

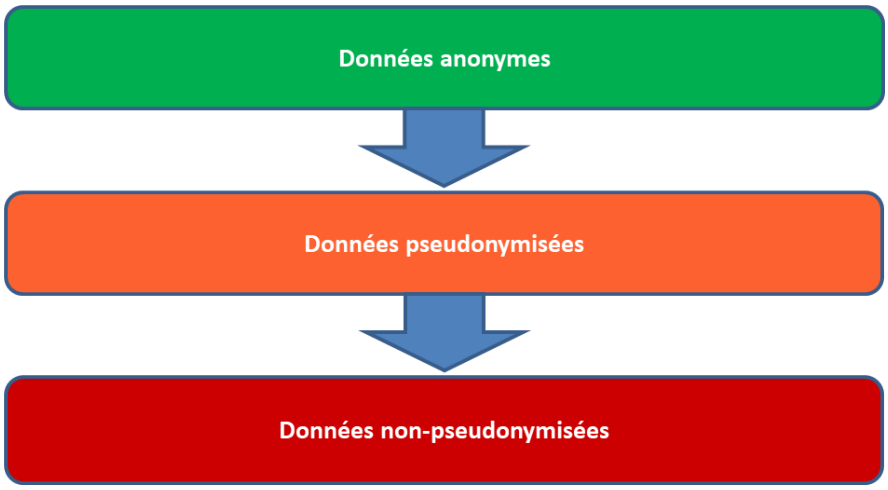
> *"la finalité ne peut induire une atteinte disproportionnée aux intérêts de la personne concernée par les données, au nom des intérêts poursuivis par le responsable du traitement. La notion de légitimité invite donc à un examen de proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées"*[26].

La détermination de la finalité permettra également de définir une durée de conservation

C. NECESSITE / PROPORTIONNALITE

Il est essentiel que seuls les traitements nécessaires à atteindre une finalité déterminée soient entrepris et que, en corollaire, seules les données nécessaires à ces traitements.

Ce principe est également appelé celui de minimisation qui peut se traduire, au niveau des données comme suit :



En d'autres termes, un responsable du traitement ne pourra traiter des données pseudonymisées qu'à la seule condition que les données anonymes ne suffisent pas à atteindre la finalité déterminée préalablement. Il en va de même pour l'utilisation de données non-pseudonymisées par rapport aux données pseudonymisées.

Ces principes de nécessité et de proportionnalité sont consacrés en Tunisie par l'article 49 de la constitution de 2014 qui affirme que : « Sans porter atteinte à leur substance, la loi fixe les restrictions relatives aux droits et libertés garantis par la Constitution et à leur exercice. Ces restrictions ne peuvent être établies que pour répondre aux exigences d'un Etat civil et démocratique, et en vue de sauvegarder les droits d'autrui ou les impératifs

[25] C. de Terwangne, "Les cabinets d'avocats et la loi sur la protection des données à caractère personnel", *Cabinet d'avocats et technologies de l'information : balises et enjeux*, 2005, p. 157.
[26] C. de Terwangne, "Les cabinets d'avocats et la loi sur la protection des données à caractère personnel", *Cabinet d'avocats et technologies de l'information : balises et enjeux*, 2005, p. 157 avec notes infrapaginales.

de la sûreté publique, de la défense nationale, de la santé publique ou de la moralité publique tout en respectant la proportionnalité entre ces restrictions et leurs justifications … ».

D. QUALITE DES DONNEES

Pour qu'un traitement soit efficace mais aussi respectueux de chaque individu dont les données sont traitées, il est fondamental que ces données soient, outre le fait d'être nécessaires, complètes et mises à jour. La personne concernée a, grâce à son droit d'accès, un droit de regard et, le cas échéant, de rectification.

Cela démontre à suffisance le caractère essentiel de la qualité des données.

E. CATEGORIES DE DONNEES

Certaines législations, telle que la Convention 108+ et le RGPD distinguent deux catégories de données dont le traitement a, en corollaire, des bases de licéité différentes.

1. DONNÉES « NORMALES »

La première catégorie est celle que nous appellerons normales dès lors que les données y reprises ne sont pas susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée. Il s'agit d'une catégorie "par défaut" dès lors que s'y retrouvent toutes les données qui ne sont pas classées comme sensible ou appartenant à des catégories particulières. Nous y retrouvons donc les noms, prénoms, adresse,…

2. DONNÉES SENSIBLES

Le deuxième type de catégories concerne les données que l'on qualifiera de sensibles ou appartenant à des catégories spéciales. Le régime habituellement mis en place est celui d'interdiction de traitement compte-tenu du fait que les données visées sont susceptibles *in se* de porter atteinte aux libertés fondamentales. Cette interdiction doit cependant connaître des exceptions qui doivent être, d'une part, précises et, d'autre part, analysées de manière stricte. A ce stade-ci de la réflexion, il nous paraît utile de relever l'ambiguïté des articles 6 et 7 par rapport à leur qualification même. En effet, ces deux articles sont applicables dès l'instant où un traitement porte sur les données visées même si le traitement ne vise pas les données à caractère personnel pour ce qu'elles sont.

Les données appartenant à cette catégorie sont généralement :

- celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale,
- les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Il faut cependant veiller à être attentif au fait que des données sensibles peuvent ne pas être traitées pour ce qu'elles révèlent ou contiennent. Par exemple, le site Internet d'une société comprend un annuaire des personnes travaillant en son sein ; annuaire

accompagné de leurs photos. Si un des employés apparaît sur la photo en portant des signes religieux, le traitement de cette photo concernerait une donnée sensible dès lors que la donnée est relative à l'appartenance religieuse de la personne concernée alors qu'il importe peu au responsable de traitement que cette personne soit d'une religion ou d'une autre. L'on devrait pouvoir considérer que les données, dans ce contexte, ne sont pas sensibles.

F. CONFIDENTIALITE ET SECURITE

La Cour européenne des droits de l'homme considère que la confidentialité et la sécurité sont des éléments essentiels. Elle a ainsi considéré que :

> *"La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (arrêt Z c. Finlande du 25 février 1997, Recueil des arrêts et décisions 1997-I, p. 347, § 95)"*[27]

1. NIVEAU ORGANISATIONNELLE

D'un point de vue organisationnel, le responsable du traitement doit s'assurer que les personnes agissant sous son autorité soient informées des dispositions de la législation relative à la protection des données à caractère personnel.

Il doit également veiller à mettre en place une structure ou une organisation pour éviter la perte de données, des destructions ou modifications de données non autorisées, des accès non autorisés, etc. En d'autres termes, il devra prendre des dispositions en termes d'organisation qui garantira la personne concernée contre de tels faits.

Ce niveau organisationnel se retrouve également au stade de la formation des personnes à n'accéder qu'aux données à caractère personnel dont elles ont réellement besoin. Par exemple, en matière de données relatives à la santé, le responsable de traitement devra s'assurer que son personnel médical n'accèdera que, d'une part, aux données des patients dont ils assurent le suivi thérapeutique et, d'autre part, aux seules données de ces patients dont ils ont besoin dans le cadre du suivi thérapeutique.

2. NIVEAU TECHNIQUE

Au niveau technique, le responsable du traitement devra s'assurer qu'il a mis en place des mesures adéquates de protection de ses traitements d'un point de vue technique et que son système informatique réunit les conditions nécessaires à éviter toute intrusion non autorisée via une bonne gestion d'accès, toute perte, destruction ou modification de données, etc.

A noter, que la notion de sécurité s'entend aussi des accès physiques au réseau informatique du responsable de traitement. Il faudra donc être attentif à ce que l'accès au serveur, par exemple, soit réglementé et n'ouvert qu'aux seules personnes qui en ont la

[27] CEDH, M. S. c. Suède (74/1996/693/885), 27.08.1997, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-62738, § 41.

nécessité. Il serait bien inutile de prévoir des règles d'accès strictes aux données si le serveur les contenant n'était pas suffisamment protégé et pouvait être subtilisé…

G. ACCOUNTABILITY

Le principe d'accountability devient un élément essentiel dans les régimes de protection des données à caractère personnel et il faut nécessairement en tenir compte. Par accountability l'on entend la responsabilité du responsable du traitement sur l'ensemble du processus de traitement des données.

H. DROITS DES PERSONNES CONCERNEES

En vertu d'un principe d'autodétermination informationnel, la personne détient un certain nombre de droits lui permettant s'assurer un contrôle sur les traitements effectués sur les données le concernant. Ces droits vont de celui d'accès à celui d'effacement en passant par les droits d'opposition, de rectification et de portabilité. Il est cependant à noter que l'exercice de certains de ces droits peut être limité.

I. PROTECTION DES DONNEES DES LA CONCEPTION ET PROTECTION DES DONNEES PAR DEFAUT

Le RGPD a introduit une notion qui, si elle était déjà connue, devient une obligation pour le responsable du traitement qui doit, dès la conception d'un traitement, s'assurer qu'il intègre les principes de protection des données.

Par ailleurs, il doit s'assurer par défaut la minimisation des données, en ce compris la durée de conservation.

J. SANCTION ET AUTORITE DE CONTROLE

Une loi sans sanction est vouée à des violations et à l'oubli. En effet, une loi n'a de pouvoir que si toute violation est suivie d'une sanction. Il s'agit d'une fonction dissuasive de la loi.

Par ailleurs, cette sanction doit toucher l'activité de la personne qui la viole. C'est ainsi que toute législation relative à la protection des données à caractère personnel doit prévoir des sanctions dissuasives à même de limiter, autant que faire se peut, les violations.

Allant de pair avec ce régime de sanctions, une autorité de contrôle doit être mise en place et doit posséder des instruments de sanction ou des instruments dont l'exercice peut mener à des sanctions.

K. FLUX TRANSFRONTIERE

Croire que les données à caractère personnel resteront dans les limites d'un territoire donné est un leurre que l'on ne peut pas se permettre de cautionner dans un texte relatif aux données à caractère personnel.

L'on doit donc nécessairement prévoir des hypothèses de flux transfrontières qui permettent un maintien de la protection des données traitées.

IV. LA PROTECTION DES DONNÉES PERSONNELLES EN TUNISIE

A. CADRE JURIDIQUE

Même si cela est peu connu du citoyen, le souci de la protection des données à caractère personnel a conduit en **1981** à l'édiction de la Circulaire du Premier ministre n° 31 du 23 novembre 1981 portant sur l'usage de la carte d'identité nationale dans l'administration publique. Ce texte interdisait clairement aux structures publiques de demander dans ses rapports avec les usagers une copie de la carte d'identité. Il leur demandait de se limiter à transcrire le numéro de la carte et sa date de délivrance dans le dossier de la prestation.

Les premières dispositions juridiques qui ont traité en Tunisie clairement de la protection des données personnelles sont les articles 38, 41 et 42 de la loi n° **2000**-83 du 9 août 2000 relative aux échanges et au commerce électroniques. Des dispositions aujourd'hui abrogées.

En **2002**, la constitution tunisienne dans sa révision de 'article 9 introduisit la protection des données personnelles en prescrivant que *"l'inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garantis, sauf dans les cas exceptionnels prévus par la loi"*. Ainsi la Tunisie était le 28e Etat dans le monde à constitutionnaliser la protection.

En **2004**, en application de la constitution, la Tunisie adopta la loi organique n° 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel. Une loi qui comporte 105 articles et constitue un réel code de la protection. Cette loi fit de la Tunisie un Etat précurseur dans sa région aussi bien arabe qu'africaine. L'article 1er précise ainsi que *"toute personne a le droit à la protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la constitution et ne peuvent être traitées que dans le cadre de la transparence, la loyauté et le respect de la dignité humaine et conformément aux dispositions de la présente loi."*. La loi reprend de nombreux principes énoncés ci-dessus et institue une autorité de contrôle indépendante étant l'Instance nationale de protection des données (INPDP, en abrégé) dotées de pouvoirs de contrôle mais également réglementaire. Le décret n°2007-3003 du 27 novembre 2007 a fixé les modalités de fonctionnement de l'INPDP qui a réellement commencé ses travaux en avril 2009 (date de la tenue de son premier conseil) suite à la désignation de ses membres en 2008. Une instance qui est la doyenne des instances de contrôle dans le monde arabe et en Afrique.

En **2014**, la nouvelle Constitution rappelle, en son article 24, que *"L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances, des communications et des données personnelles. (…)"*.

D'un point de vue international, la Tunisie ratifie la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel en **2017** par la loi organique n° 2017-42 du 30 mai 2017, portant approbation de l'adhésion de la République Tunisienne à la convention n° 108 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 n° 181 concernant les autorités de contrôle et les flux transfrontières de données. Elle en a été en octobre 2017 le 51e membre, le quatrième en dehors du conseil de l'Europe après l'Uruguay, l'Ile Maurice et le Sénégal. Une convention qui prend une place supérieure à la loi organique de 2004 dans l'ordonnancement des textes juridiques nationaux et ce conformément à l'article 20 de la Constitution de 2004. Cette place conduit à la révision implicite de plusieurs dispositions de la loi et notamment les articles 4 (Définition des données personnelles), 16 (le traitement des données par les employeurs) mais surtout les articles 53 et 54 (traitement des données personnelles par les personnes publiques).

La loi tunisienne n'a jamais été formellement révisée depuis son édiction malgré l'évolution fulgurante des techniques de traitement des données et surtout porte en elle des malformations congénitales, induites par le cadre de son édiction qui était celui d'un régime politique loin d'être protecteur des droits et des libertés mais qui devait démontrer à la société internationale qu'il était apte à héberger les travaux du sommet mondial sur la société de l'information qu'il hébergeait en 2005.

Pour toutes ces raisons et surtout suite à l'édiction du RGPD européen qui entrait en application le 25 mai 2018, la Tunisie rédigea un nouveau projet de loi organique relatif à la protection des données à caractère personnel qui fut transmis au Parlement en mars **2018**. Ce projet modernise la loi de 2004 afin d'y intégrer les évolutions technologiques survenues depuis la publication de la loi de 2004 et intégrer certains principes internationaux relatifs à la protection des données à caractère personnel.

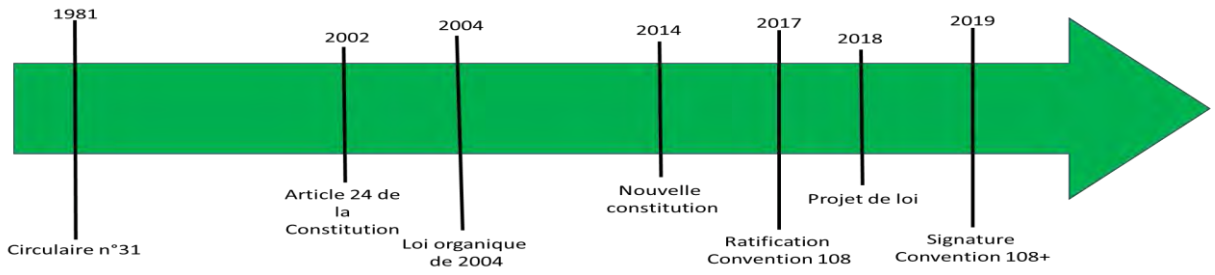
En **2019**, la Tunisie signe la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel consolidée à la lumière du protocole additionnel (Convention 108+).

Mais la Tunisie à côté de sa constitution, de la convention et de sa loi organique appliquée à travers ses deux décrets d'application de 2017 a étoffé son corpus juridique dans ce domaine. Deux circulaires du Chef du Gouvernement ont été édictées la première en **2016** rappelant aux structures publiques le nécessaire respect de la constitution et de la loi organique et la circulaire de **2019** qui traite de la manière avec laquelle on doit traiter les données de la carte d'identité nationale.

Mais le corpus juridique a vu un développement remarquable de la présence de la protection des données personnelles dans plus de 17 lois organiques et ordinaires, quelques 16 décrets et arrêtés relatifs à divers domaines d'activités.

Enfin, l'INPDP conformément aux missions qui lui sont impartis par la loi de 2004 a édicté depuis **2016** cinq délibérations qui ont un caractère réglementaire : La numéro 2 (2017) relative à l'activité politique, la numéro 3 (2018) déterminant les Etats qu'elle considère comme ayant une protection adéquate, la délibération numéro 4 (2018) relative aux données de santé, celle portant le numéro 5 (2018) relative à la vidéoprotection et enfin la dernière la numéro 6 (2019) relative aux opérations de contrôle.

Par ailleurs, le Président de l'INPDP est, depuis septembre **2019**, Président de l'Association francophone des autorités de protection des données, et ce, pour trois ans.



L'on constate, à la lecture de cet historique, que la Tunisie a toujours eu la volonté de protéger les données à caractère personnel. Elle démontre aujourd'hui qu'elle veut se placer dans la cadre des normes internationale dans la matière. Le projet de loi actuellement au Parlement est ainsi plus important que la loi actuellement en vigueur. C'est la préfiguration du corpus qu'aura la Tunisie dans quelques temps.

B. L'INPDP

A l'image de toutes les structures chargées de la protection des données personnelles dans les expériences comparées, l'INPDP a été installée fin de l'année 2008. La loi organique de 2004 lui attribue les missions suivantes :

- Reçoit les déclarations et les demandes d'autorisation de traitement des données ;
- Reçoit les plaintes qui portent sur les violations des normes de protection ;
- Répond aux demandes d'avis sur la protection des données ;
- Statue sur les violations et prend les décisions pour les arrêter dont les décisions d'arrêt de traitement ou le retrait de la décision d'autorisation ;
- Détermine les garanties nécessaires ainsi que les mesures appropriées à mettre en œuvre pour assurer la protection des données et élabore les règles de conduites ce qui la fait bénéficier d'un pouvoir réglementaire propre ;
- Réaliser toutes les missions de contrôle et d'investigation portant sur le traitement des données personnelles.

Depuis 2009, l'Instance au statistiquement réalisé les activités chiffrées suivantes :

	5	4			3			2			1			Mandat المدة
	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009	Année السنة
4600	328	511	573	934	637	530	542	62	116	65	127	170	5	Vidéosurveillance مراقبة بصرية
1304	157	269	313	140	196	83	63	8	8	17	15	29	6	Déclarations تصاريح المعالجة
687	88	115	135	118	103	61	34	8	6	9	2	5	3	Transfert étranger نقل الى الخارج
531	73	117	112	106	44	41	17	8	2	5	3	2	1	Plaintes شكايات
401	54	80	78	69	62	29	28	---	---	1	---	---	---	Santé صحة
362	29	56	75	48	116	37	1	---	---	---	---	---	---	Biométrie معطيات بيومترية
259	24	94	49	25	15	11	5	9	5	10	2	5	5	Avis رأي
241	235	2	4	---	---	---	---	---	---	---	---	---	---	Contrôles الرقابة
88	23	23	13	15	11	1	---	---	2	---	---	---	---	Communication اتصال
18	---	---	1	---	17	---	---	---	---	---	---	---	---	Convictions & Appart. معتقدات وانتماءات
8491	1011	1267	1353	1455	1201	793	690	95	139	107	149	211	20	Total annuel مجموع سنوي
-	112	106	113	121	100	66	58	8	12	9	12	18	1,5	Moyenne mensuelle المعدل الشهري
-		4075			2684			341			380			Total mandat مجموع المدة

Mise à jour / تحيين : 17-08-2021

Ainsi, il apparait des chiffres que l'Instance a traités une dizaine de dossier par mois d'activité depuis 2009. Mais depuis 2015 et le lancement d'une activité proactive la présence médiatique et publique importante, le nombre des dossiers a été multiplié par 10 pour dépasser les 100 dossiers par mois d'activité.

Il est à remarquer que des domaines de traitement de données n'ont jamais donné lieu à des décisions de l'instance avant 2015 comme celui relatif à la santé ou la biométrie ou la communication ou enfin les convictions et les appartenances malgré qu'ils soient des traitements relatifs à des données sensibles. Les déclarations de traitement qui est la procédure de base de tout traitement est passée de dix à une moyenne de 250 dossiers par an.

Le nombre des **plaintes** était dérisoire et totalisait jusqu'en 2014 seulement 21 dossiers. Les trois dernières années (2018-2020) l'INPDP statue sur plus d'une centaine de plaintes par an. L'Instance a ainsi à la fin de l'année 2021 a atteint quelques 550 plaintes. La grande majorité, il est vrai portent sur des violations des normes de la vidéosurveillance ce qui dénote d'un manque de culture de la protection des données dans la société. Plus de la moitié des dossiers sont transmis aux Procureurs de la République territorialement compétents.

L'Instance d'après la loi de 2004 procède de deux manières concernant les constatations des violations de la loi de protection : Jusque-là l'INPD, en se basant sur l'article 77 de la loi, se limitait à informer le procureur de la République territorialement compétent de toutes les violations fondées qui lui parviennent à travers des plaintes. Dans ces cas l'Instance n'est ni plaignante, ni témoin et certainement pas faisant l'objet d'une plainte. Elle n'a de ce fait aucune qualité pour être impliqué dans la procédure judiciaire. A ce niveau l'Instance depuis 2016 a communiqué aux procureurs quelques 250 dossiers dont certains contre des entreprises publiques et privées de renom. Mais la plupart des dossiers sont en relation avec la violation des normes en matière de (vidéoprotection) vidéosurveillance. A notre connaissance aucun dossier n'a été traité ou alors la justice ne prend pas la peine d'informer l'instance du sort réservé aux dossiers qui lui sont transmis.

La première manière ayant prouvé son inefficacité, l'Instance a depuis le début de 2021 changé la manière de faire. En effet, la loi organique numéro 2004-63 dans ses dispositions donne le pouvoir à l'instance de recevoir les plaintes. Mais elle lui permet aussi de réaliser toutes les investigations nécessaires et d'ailleurs il est clairement spécifié que le secret professionnel ne peut lui être opposé. Elle peut aussi auditionner les responsables de traitement. Enfin, l'Instance a le pouvoir de prendre une décision d'interdire le traitement des données personnelles et le droit de retirer ses décisions d'autorisation de traitement. Ces décisions ayant un caractère juridictionnel, elles doivent être motivées et sont susceptibles d'appel devant la cour d'appel de Tunis.

Les **demandes d'avis** étaient très timides depuis la mise en place de l'INPDP. En effet, de 2009 à 2014 elle n'a répondu qu'à 36 demandes d'avis. Depuis 2015 elle a reçu quelques 223 dossiers. L'Instance est en train de préparer le recueil des avis de l'Instance qui sera publié avant la fin de l'année 2021.

Enfin l'Instance n'a jamais réalisé aucun **contrôle de la conformité** des traitements des données personnelles par les responsables depuis sa création. Ce n'est que depuis 2019 qu'elle a entamé ce type de missions. Jusqu'à ce jour elle a réalisé 6 missions de contrôle in situ. Depuis juin 2021, elle a entamé une action à grande échelle de contrôle sur dossier

qui a touché plus de 300 structures et publique. L'Instance accompagne les structures dans leur travail de mise en conformité et leur attribue une évaluation publique basée sur 23 critères. Suite à cette activité l'Instance a emmené les structures publiques et privées à nommer en interne un chargé de la protection maitre d'œuvre de l'opération de mise en conformité qui commence par une cartographie qui donnera lieu au registre de traitement.

L'INPDP n'a jamais réalisé de **rapport d'activité** depuis son entrée en activité. En 2018 elle présenta son premier rapport aux trois présidents. Il portait sur les années 2099 jusqu'à 2017. Aujourd'hui deux rapports sont au stade de finalisation celui de 2018 et celui de 2019.

C. LA PROTECTION DES DONNEES A TRAVERS LE PROJET DE LOI DE 2018

1. INTRODUCTION

Le nouveau projet de loi relatif à la protection des données a été déposé au Parlement tunisien et avait entamé son parcours parlementaire. Cependant, ce parcours a été interrompu par les élections intervenues en 2019 et n'a pas redémarré eu égard à la crise de la Covid 19 et la décision de gel des activités à partir du 25 juillet 2021 de l'Assemblée des Représentants du Peuple.

Le projet de loi reprend des principes internationaux importants vus ci-dessus montrant ainsi que la loi ne peut pas être lue sans avoir à l'esprit les normes internationales. De plus, le projet a, pour objectif, de moderniser la loi de 2004 afin d'y intégrer les évolutions technologiques même si le principe de neutralité technologique est préservé. Cela signifie que la loi ne privilégie pas des technologies particulières mais vise à instaurer des comportements ou des processus communs à toutes les technologies.

Le projet contient une partie fixant des définitions et des principes généraux tant au niveau, par exemple, des obligations à charges des responsables du traitement que des droits des personnes concernées. Une seconde partie est, elle, consacrée à des secteurs d'activités particuliers que sont le journalisme, la recherche médicale, les objets connectés et le big data.

2. PARTIE GÉNÉRALE

a. Champ d'application

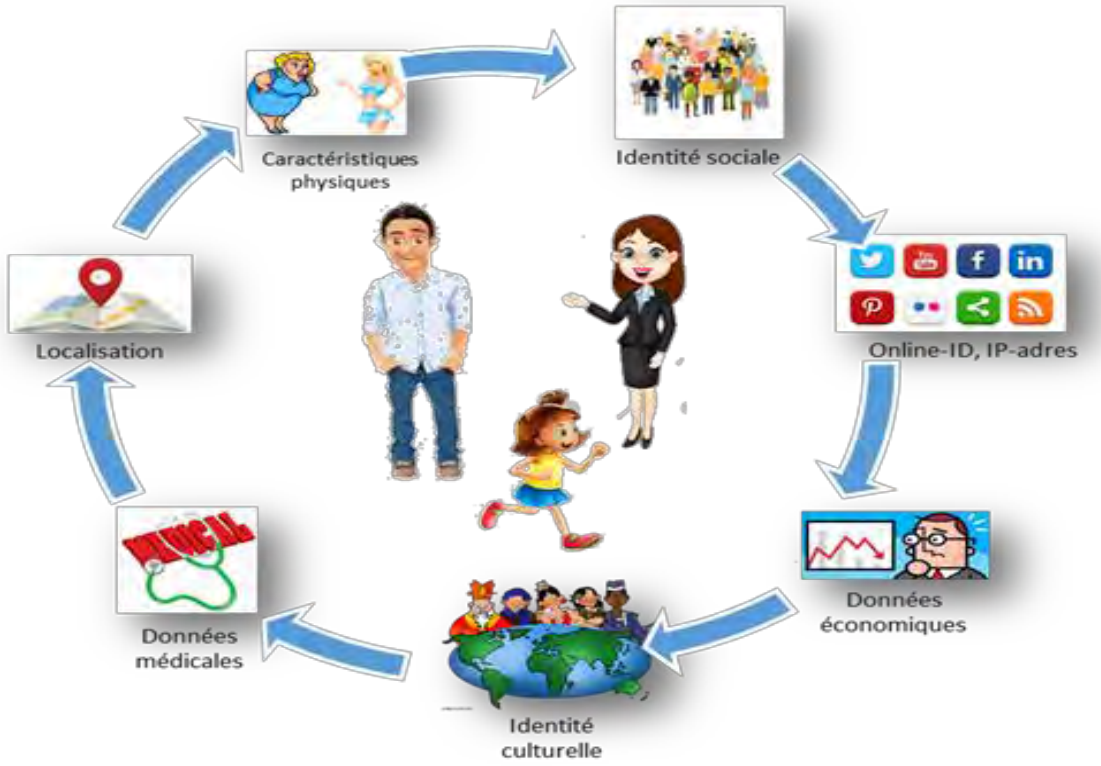
Le projet de loi se veut la plus inclusive possible en termes de protection des données à caractère personnel.

Ainsi, le projet s'applique au *"traitement automatisé et au traitement non automatisé des données à caractère personnel [à l'exception de ceux ayant pour finalité un usage personnel ou familial] mis en œuvre sur le territoire national à moins qu'il ne soit contraire aux exigences de la sûreté publique et la défense nationale conformément à la législation en vigueur."* Cela signifie que, d'un point de vue matériel, tout traitement de données à caractère personnel entre dans le champ d'application de la loi sauf ceux qui sont effectués dans le cadre d'une activité personnelle ou domestique (photos familiales,

agenda personnel, carnet d'adresse personnel, etc.) et, d'un point de vue, territorial, tout le territoire tunisien est visé.

Cette même volonté se retrouve au niveau de la définition de donnée à caractère personnel qui vise "toutes les données quelle que soit leur origine ou leur forme se rapportant à une personne physique identifiée ou identifiables, directement ou indirectement, à travers plusieurs informations ou symboles". L'utilisation du déterminant "toutes" en début de définition montre clairement cette volonté d'englober le plus d'éléments informationnels dans le concept de données à caractère personnel pouvant être le nom, le prénom, les adresses IP, un log. Des images vidéo peuvent également être considérées comme des données à caractère personnel. Nous attirons l'attention sur le fait que cette définition ne vise que les personnes physiques (personnes concernées) à l'exclusion des personnes morales. Cette limitation aux personnes physiques peut s'expliquer par le fait que la loi traite d'un droit fondamental qui, par définition, n'est l'attribut que des dites personnes physiques.

© Manon Knockaert, Crids



© Alain Brisy, Naxos IT

Il en va également de la définition de traitement qui parle de "les opérations" et dont l'énumération n'est pas exhaustive.

© Manon Knockaert, Crids

Le traitement est donc un ensemble d'opération extrêmement large. Le fait de collecter ou consulter des données à caractère personnel est déjà considéré comme un traitement de données à caractère personnel. Il en va de même lorsqu'un logiciel de traitement de texte est utilisé pour enregistrer des données à caractère personnel. A titre d'exemple, le fait, pour un gestionnaire de site Internet, d'enregistrer et conserver des données pour lui permettre d'envoyer des courriels sollicités ou non constitue un traitement de données à caractère personnel.

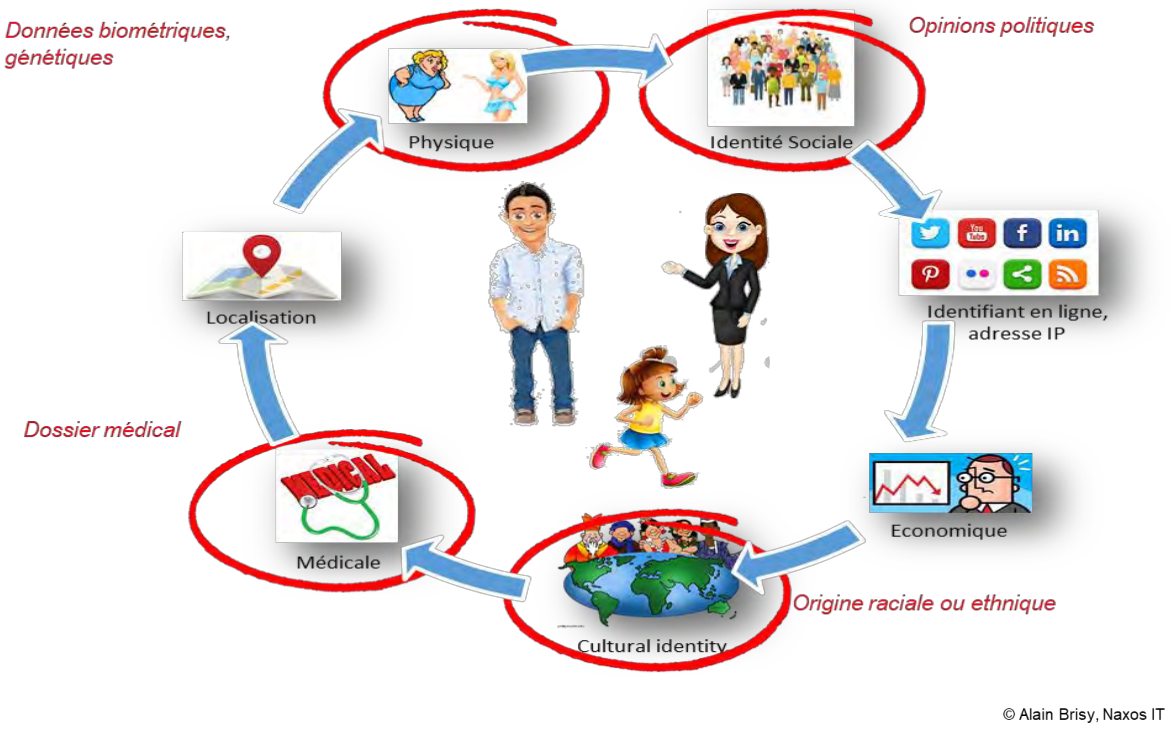
Il est également utile de relever que la notion de traitement ne s'applique pas uniquement lors d'opérations à l'aide de procédés automatisés mais également à des traitements manuels. Dans cette dernière hypothèse, il est habituellement convenu que les données soient accessibles en fonction de critères déterminés. Par exemple, un classement sur base des noms des personnes, par ordre alphabétique constitue un fichier.

La conséquence de définitions aussi larges est que la plupart des données traitées par une entreprise ou une autorité publique sont couvertes par la loi. L'on constate donc que la loi impacte de manière importante la vie économique via les entreprises mais aussi publique via les autorités publiques. Par conséquent, il est clair que la grande.

b. Catégories de données

Le projet de loi distingue, de facto, deux catégories de données. La première catégorie est celle que nous appellerons normales dès lors qu'elles suivent un régime général d'autorisation de traitement. Il s'agit d'une catégorie "par défaut" dès lors que s'y retrouvent toutes les données qui ne sont pas visées par l'article 31 du projet de loi. Nous y retrouvons donc les noms, prénoms, adresse, …

Le deuxième type de catégories concerne les données que l'on qualifiera de "sensibles" et dont le traitement est, principe, interdit en vertu de l'article 31 qui précise qu'*"est interdit le traitement des données à caractère personnel relatives à l'origine raciale ou génétique d'une personne, ou à ses convictions religieuses, ou à ses opinions et ses appartenances politiques ou philosophiques ou syndicales, ou à ses données biométriques, ou de santé ou sexuelles"*.

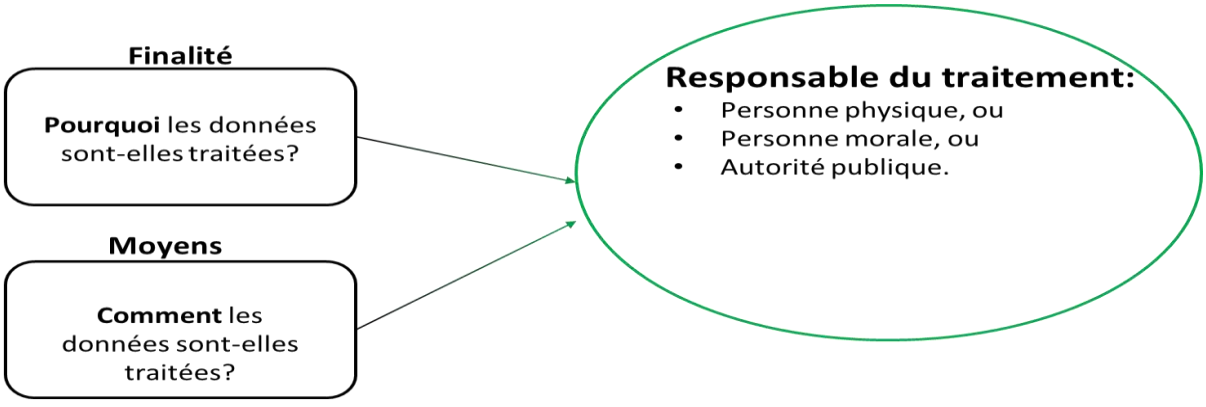


Ce régime d'interdiction de traitement tient du fait que les données visées sont susceptibles in se de porter atteinte aux libertés fondamentales ou à la vie privée. Le projet de loi prévoit des exceptions à l'interdiction qui sont principalement basées sur une base légale et sous réserve d'autorisation par l'INPDCP.

c. Les "acteurs"

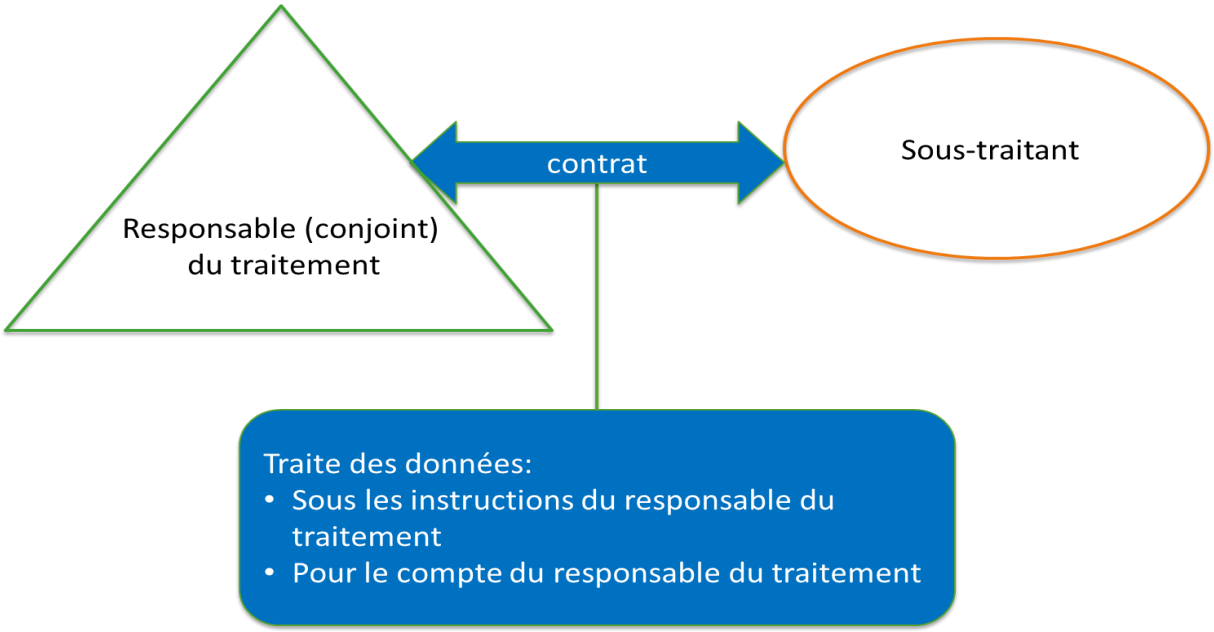
Si le premier acteur est déjà connu, à savoir la personne concernée, c'est-à-dire la personne physique identifiée ou identifiable à laquelle se rapportent les données à caractère personnel, deux autres acteurs jouent un rôle important en matière de protection des données à caractère personnel. Ce sont les responsable du traitement et sous-traitant.

L'article 4.9 du projet de loi définit le responsable du traitement comme *"toute personne physique ou morale, tunisienne ou étrangère, privée ou publique, et toute autorité publique chargées de déterminer la nature des données à caractère personnel, l'objectif du traitement et ses modalités."* En d'autres, c'est celui qui va fixer le "pourquoi" du traitement mais également le "comment" pour parvenir.



Le projet de loi impose que le responsable du traitement soit établi en Tunisie.

Bien souvent, le responsable du traitement fera appel aux services d'un sous-traitant qui est *"toute personne physique ou morale publique ou privée qui traite des données à caractère personnel pour le compte et sous le contrôle du responsable du traitement."* (Article 4, 11 du projet de loi). En d'autres termes, le sous-traitant n'a aucune autonomie décisionnelle dès lors qu'il devra exécuter les tâches assignées par le responsable du traitement. Un contrat devrait être conclu entre les deux parties.



d. Transparence

Le responsable du traitement doit être assurer une transparence à l'égard de la personne concernée. Cette transparence est mise en œuvre par divers moyens :

- Information délivrée à la personne concernée. Cela implique que les informations doivent être correctes mais aussi pertinentes par rapport à l'objectif déterminé et déclaré du traitement. Il faut mettre en œuvre le principe selon lequel on ne peut collecter et traiter que les données à caractère personnel nécessaires à cette finalité.
- Une déclaration du traitement auprès de l'INDPDP et, le cas échéant, une demande d'autorisation (principalement pour un traitement de données sensibles).
- Le droit d'accès au traitement accordé à la personne concernée ; droit duquel découlent toute une série d'autres droits tels que ceux de rectification, suppression, portabilité. A noter que ce droit d'accès englobe le droit de recevoir une copie des données concernant la personne concernée qui sont traitées.

e. Sécurité

L'article 37 du projet de loi impose au responsable du traitement et au sous-traitant de prendre toutes les mesures nécessaires pour assurer la sécurité des données et empêcher les tiers de les consulter, modifier ou altérer. De manière assez classique, il faut voir la sécurité à deux niveaux, à savoir aux niveaux organisationnel et technique.

D'un point de vue organisationnel, le responsable de traitement et le sous-traitant doivent s'assurer que les personnes agissant sous leur autorité soient informées des dispositions

du projet de loi. Il doit également veiller à mettre en place une structure ou une organisation pour éviter la perte de données, des destructions ou modifications de données non autorisées, des accès non autorisés, etc. En d'autres termes, il devra prendre des dispositions en termes d'organisation qui garantira la personne concernée contre de tels faits. Par exemple, le responsable de traitement devra s'assurer que seules les personnes devant effectivement avoir accès à des données à caractère personnel y ait effectivement accès à l'exclusion des autres. Il lui appartiendra donc de prévoir une organisation adéquate et efficace. Cette notion de sécurité organisationnelle peut également être expliquée à travers l'exemple de l'utilisation des mots de passe pour accéder à un réseau protégé. Il a été constaté que certaines entreprises imposent à leurs employés de changer de mot de passe tous les mois sans pouvoir choisir un mot de passe qu'ils auraient déjà utilisé durant les six derniers mois. Si le principe peut paraître intéressant pour éviter l'usurpation d'identité sur le réseau informatique de la société, cela s'avère, en réalité une catastrophe. En effet, l'on constate que les employés écrivent leur mot de passe sur un papier collé à leur ordinateur pour être certain de ne pas l'oublier compte-tenu du rythme de changement de mot de passe imposé. Cette organisation au niveau des mots de passe est donc totalement contre-productive dès lors que le système information n'est plus protégé de manière efficace et le responsable de traitement contreviendrait donc à son obligation de sécurité sans s'en rendre compte.

Le niveau organisationnel se retrouve également au stade de la formation des personnes à n'accéder qu'aux données à caractère personnel dont elles ont réellement besoin. Par exemple, en matière de données relatives à la santé, le responsable de traitement devra s'assurer que son personnel médical n'accèdera que, d'une part, aux données des patients dont ils assurent le suivi thérapeutique et, d'autre part, aux seules données de ces patients dont ils ont besoin dans le cadre du suivi thérapeutique.

Au niveau technique, le responsable de traitement et le sous-traitant devront s'assurer qu'ils ont mis en place des mesures adéquates de protection de leurs traitements d'un point de vue technique. Ainsi, ils devront s'assurer que leur système informatique réunit les conditions nécessaires à éviter toute intrusion non autorisée via une bonne gestion d'accès, toute perte, destruction ou modification de données, etc. A noter, que la notion de sécurité s'entend aussi des accès physiques au réseau informatique du responsable de traitement et du sous-traitant. Il faudra donc être attentif à ce que l'accès au serveur, par exemple, soit réglementé et n'ouvert qu'aux seules personnes qui en ont la nécessité. Il serait bien inutile de prévoir des règles d'accès strictes aux données si le serveur les contenant n'était pas suffisamment protégé et pouvait être subtilisé…

A noter que le projet de loi impose une étude de risques de manière périodique.

f. Droits des personnes concernées

La personne concernée a toute une série de droits qui sont une mise en œuvre de son droit à l'autodétermination informationnelle.

Nous avons déjà rencontré le droit d'accès mais à celui s'ajoutent :

- Droit d'opposition fondé sur les motifs pertinents et légitime. A noter que ce droit d'opposition ne pourra être déclaré recevable si le traitement se fonde sur une loi dès lors que le responsable ne fait que répondre à une obligation légale.
- Droit à la portabilité permet à la personne concernée de demander à un responsable du traitement traitant les données le concernant de les transférer à un autre responsable du traitement qu'il désigne.

- Droit à l'oubli et au déréférencement permet à la personne concernée de demander l'effacement des données la concernant pour 4 motifs (article 24 du projet de loi):
    - Si le traitement des données à caractère personnel a été fait sous une forme ou pour une finalité autre que celles pour lesquelles elles ont été collectées ;
    - Si la personne concernée par le traitement a retiré le consentement sur lequel est fondé le traitement ;
    - Si les données à caractère personnel ont fait l'objet d'un traitement illicite ;
    - Si les données à caractère personnel devaient être supprimées suite à l'exécution ou l'extinction d'une obligation juridique ou contractuelle à laquelle le responsable du traitement est soumis.

Ce droit à l'oubli ne peut cependant pas s'exercer si le traitement est nécessaire pour (article 27 du projet de loi):

- Respecter des exigences légales que requiert la continuité du traitement ;
- Des motifs d'intérêt public dans le domaine de la santé
- Des fins archivistiques dans l'intérêt public, de recherche scientifique ou historique ou statistique.
- La constatation des droits, leur exercice ou leur défense en justice.

Par ailleurs, la personne concernée peut demander "à tout responsable d'un moteur de recherche national de supprimer le lien avec le résultat de recherche lié à son nom et prénom et le responsable est tenu d'effectuer la suppression" (article 28 du projet de loi). L'on doit cependant souligner que ce *"déférencement n'implique pas la suppression des données de la source"* (article 28 du projet de loi).

g. L'Instance nationale de protection des données à caractère personnel

L'INPDCP est une autorité de protection des données indépendante. Cela signifie qu'elle ne reçoit d'instruction d'aucun pouvoir politique ou autorité publique.

Ses missions essentielles sont de veiller au respect du projet de loi mais aussi assurer une sensibilisation à la protection des données à caractère personnel. Par ailleurs, elle procède à une certaine publicité des traitements.

Elle peut être saisie par toute personne concernée qui estimerait que les données à caractère personnel la concernant sont traitées d'une manière qui n'est pas conforme au projet de loi.

h. Sanctions

Le projet de loi prévoit des sanctions prononcées par l'INPDCP ou pénales prononcées par une juridiction judiciaire en cas d'infraction. Ces sanctions y sont reprises aux articles 104 à 117.

Une des sanctions est l'arrêt immédiat du traitement qui paraît, en réalité, la plus efficace dans le chef d'entreprises ou d'autorités publiques.

3. LES MATIÈRES PARTICULIÈRES

Le projet de loi prévoit des régimes particuliers pour des secteurs particuliers pour lesquels une adaptation des règles doit avoir lieu

a. Du traitement des données à caractère personnel relatives à la sécurité publique ou la défense nationale ou les poursuites pénales

Ces données sont, dans certaines législations, classées comme "sensibles", choix qui est effectué par le projet de loi. Compte-tenu de ce caractère particulièrement sensible mais également du fait que ces traitements touchent à la sécurité de la société, le droit d'accès par la personne concernée est modifié puisqu'il perd son caractère direct pour devenir indirect. En effet, la personne concernée doit passer par un membre de l'Instance pour les traitements liés à la sécurité publique ou la défense nationale ou par un avocat désigné par la personne concernée pour les traitements liés aux poursuites pénales pour accéder aux données traitées.

La demande est alors analysée par l'Instance qui autorisera l'accès si *"le traitement aux données à caractère personnel ne s'oppose pas aux finalités du traitement et ne porte pas atteinte à la sécurité publique ou la défense nationale"* (article 53 du projet de loi). A noter que le responsable du traitement peut s'opposer à la demande et, en cas de litige, il revient à l'Instance de statuer.

b. Du traitement des données à caractère personnel à des fins de vidéosurveillance

Les caméras de vidéosurveillance constituent une réelle intrusion dans la vie privée des personnes de sorte que leur installation et leur utilisation sont strictement réglementées par le projet de loi.

Ainsi, *"les moyens de vidéosurveillance ne peuvent être utilisés que s'ils sont nécessaires pour assurer la sécurité des personnes, la prévention des accidents, la protection des biens ou l'organisation des mouvements d'entrée et de la sortie dans les espaces publics à condition qu'ils ne soient installés qu'après notification faite à l'Instance"* (article 54 du projet de loi).

De plus, ils ne peuvent être installés que dans des lieux précisés par le projet de loi, à savoir les espaces ouverts au public et leurs entrées, les espaces de transport terrestre, maritime, aérien des voyageurs et des marchandises ainsi que les abris et les lieux de travail collectif.

En outre, les enregistrements vidéo ne peuvent être accompagnés d'enregistrements sonores sauf si les moyens de vidéosurveillances sont utilisés par *"les agents de l'Etat ou des collectivités locales"* (article 54 du projet de loi) et après notification à l'Instance.

Les établissements sécuritaires ou militaires ne peuvent pas être couverts par moyens de vidéosurveillance. Par contre, *"l'installation des moyens de vidéosurveillance dans les milieux d'enseignement, de santé ou dans les cellules de garde à vue et dans les prisons et les centres de réhabilitation est soumises à l'autorisation préalable de l'Instance"* (article 55 du projet de loi).

Une notification auprès de l'Instance est également requise pour l'installation de moyens de vidéosurveillance sur la voie publique par les autorités publiques ainsi que, d'une part, le recours à de tels moyens installés par des particuliers par les autorités chargées de la sécurité publique ou de la défense nationale et, d'autre part, *"la reconnaissance faciale des personnes physiques ou par les plaques d'immatriculation des véhicules réalisée par les services publics ou privés à travers les enregistrements issus des systèmes de vidéosurveillance installés conformément à la législation en vigueur"* (article 59 du projet de loi).

En termes de communication des enregistrements, un régime d'interdiction est institué avec les exceptions suivantes qui donnent lieu à une inscription de toute communication dans un registre spécial :

Lorsque la personne concernée a donné son consentement ou à sa demande ;

Lorsque la communication est nécessaire à l'exercice des missions de sécurité publique ou de défense nationale dévolues aux autorités publiques ;

Lorsque la communication s'avère nécessaire pour la constatation ou la divulgation des infractions pénales ou la poursuite des auteurs de ces infractions.

L'on constate que ces diverses mesures particulières ont pour objectif de protéger les citoyens contre d'éventuelles intrusions dans leur vie privée via des caméras de vidéosurveillance et ainsi remettre une proportionnalité entre les intérêts du responsable du traitement et la personne concernée.

c. Du traitement des données à caractère personnel relatives à la santé

Les données santé sont considérées par le projet de loi comme des données sensibles en son article 31 avec le régime d'interdiction de traitement qui l'accompagne. Les articles 60 et suivants du projet de loi fixent cependant les règles sur base desquelles un traitement est possible.

Tout traitement de données à caractère personnel relative à la santé doit faire l'objet d'une autorisation de l'Instance. Par ailleurs, seuls les traitements suivants sont autorisés (article 61 du projet de loi) :

Lorsque le traitement est réalisé par une structure publique ou privée de santé ou un personnel de santé dans le cadre de l'exercice de ses missions ;

Lorsque le traitement est nécessaire à la réalisation de finalités prévues par la loi ;

Lorsque le traitement s'avère nécessaire pour le développement et la protection de la santé entre autres pour la recherche sur les maladies et leur prévention et traitement ;

Lorsqu'il est bénéfique pour la santé de la personne concernée.

Afin de renforcer la protection de telles données, le projet de loi précise que leur traitement doit être effectué *"par des médecins et le personnel paramédical exerçant sous leur responsabilité, ou des personnes soumises, en raison de leur fonction dans le domaine médical, à l'obligation de secret professionnel"* (article 62 du projet de loi).

De plus, de telles données ne peuvent être hébergées hors du territoire tunisien et l'hébergeur en Tunisie doit avoir été agréé préalablement.

d. Du traitement des données à caractère personnel dans le cadre de la recherche scientifique

Le projet de loi rappelle et met en application le principe de minimisation en précisant qu'*"il faut procéder à la pseudonymisation et l'anonymisation, à chaque fois que les exigences de la recherche scientifique le permettent, et ce, conformément aux procédures fixées par une décision de l'Instance"* (article 64 du projet de loi).

La communication de telles données est également réglementée de sorte qu'elle *"ne peut avoir lieu que lorsque la personne concernée donne son consentement exprès ou lorsque la communication s'avère nécessaire pour la présentation des résultats de cette recherche"* (article 65 du projet de loi).

e. Du traitement des données à caractère personnel à des fins de journalisme

Le principe mis en place afin de garantir la protection des données des citoyens est celui de l'interdiction de *"rendre publiques des données à caractère personnel qui peuvent rendre les personnes concernées identifiées ou identifiables et dont ils ont pris connaissance à l'occasion de leur investigation"* (article 66 du projet de loi). Le régime est encore plus strict pour les données sensibles et relatives aux mineurs puisque leur divulgation-même est interdite.

f. Du traitement des données à caractère personnel de localisation

Le principe de nécessité de traitement est rappelé dès lors que de telles données de localisation ne peuvent être traitées que si cela est nécessaire et le traitement doit être notifié à l'Instance.

De plus et dans l'hypothèse où un tel traitement est mis en place à l'égard d'agent du responsable du traitement ou du sous-traitant lors de l'exercice de son travail, cet agent doit en être informé.

Si un tel traitement fait appel à des objets connectés, ses conditions de mise en œuvre sont fixées par l'Instance *"après consultation des structures chargées de contrôle et de régulation dans le domaine des télécommunications électroniques"* (article 69 du projet de loi).

g. Du traitement des données personnelles par le biais des objets connectés

Le projet de loi prend en compte le pouvoir invasif des objets connectés en mettant en place un régime particulier pour ceux qui sont importés ou fabriqués en Tunisie. Ainsi, ils sont soumis à certification et doivent respecter les règles de protection des données à caractère personnel applicables. A noter que les conditions de protection sont fixées par décision de l'Instance qui aura, préalablement, consulté les structures chargées de contrôle et de régulation dans le domaine des télécommunications électroniques.

h. De l'hébergement des données à caractère personnel

L'hébergement des données est un domaine en pleine expansion et le projet de loi entend fixer certaines règles en vue d'assurer une protection des données à caractère personnel effective.

Le projet de loi prévoit des règles de localisation différentes selon que l'hébergement soit opéré par une autorité publique ou par un entrepreneur privé. Dans la première hypothèse, l'hébergement doit être localisé sur le territoire tunisien tandis que, dans la seconde hypothèse, l'hébergement peut être localisé hors du territoire tunisien à condition de respecter les règles fixées par l'article 46 du projet de loi concernant les flux de données hors de la Tunisie.

En outre, le projet de loi dispose que l'hébergeur doit être considéré comme sous-traitant avec, comme conséquence, une solidarité entre responsable du traitement et sous-traitant.

L'on rappelle également que l'hébergement de données relatives à la santé hors du territoire tunisien est interdit (cf. ci-dessus).

i. Des décisions automatisées et du profilage

Le développement des technologies offre de larges possibilités de débouchés dont l'intelligence artificielle sur laquelle certains acteurs se reposent pour prendre des décisions automatisées pouvant impacter de manière importante les personnes concernées.

Afin de les prémunir contre ces effets négatifs, le projet de loi dispose que la personne concernée peut exercer son droit d'opposition prévu aux articles 20 et 21 du projet de loi et ainsi s'opposer à *"une décision fondée exclusivement sur un traitement automatisé et les effets juridiques qui s'en produisent à moins que le traitement ne soit nécessaire pour l'exécution d'une obligation juridique ou contractuelle"* (article 74 du projet de loi).

j. Du registre de l'identifiant unique du citoyen

Un décret-loi relatif à un identifiant unique du citoyen a été pris en 2020. Il s'agit d'attribuer, à tout citoyen tunisien, un identifiant composé de 11 chiffres qui le suivra durant toute sa vie.

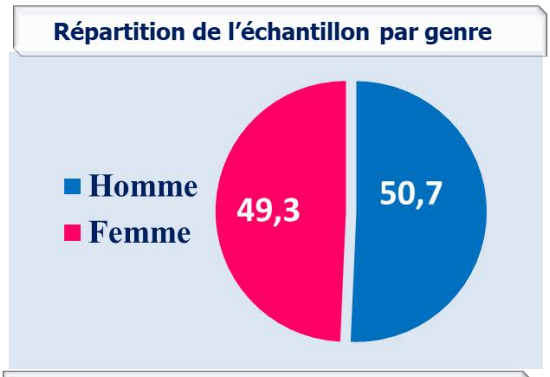
Parallèlement à la mise en place d'un tel identifiant, un registre est créé dans le respect des règles de protection des données à caractère personnel applicable et *"dont les objectifs et les données à caractère personnels qu'il pourrait comprendre sont fixés par un décret gouvernemental"* (article 75 du projet de loi). Un tel registre peut faire l'objet de contrôle de la part de l'Instance et il est même prescrit que les personnes habilitées à utiliser le "Registre de l'identifiant unique du citoyen" doivent faciliter cette mission. De plus, ces mêmes personnes doivent désigner un chargé de protection des données à caractère personnel.

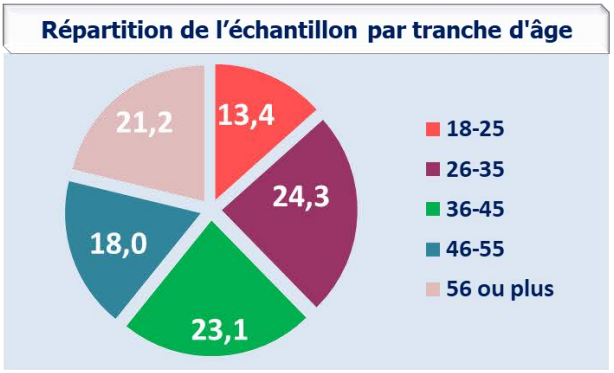
Le projet de loi fixe les règles d'attribution de l'identifiant unique du citoyen et la durée de conservation des Données à caractère personnel de 30 ans à partir du décès de la personne ou de sa déchéance de nationalité.

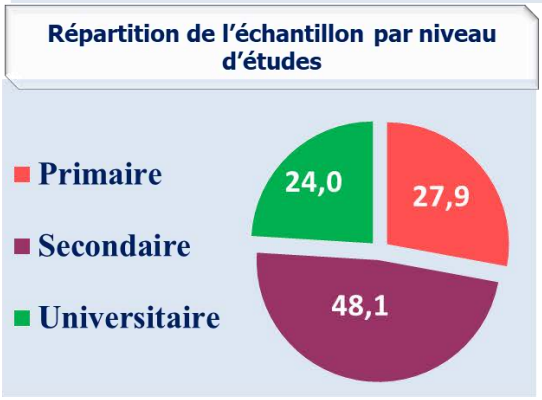
V. La culture de la protection

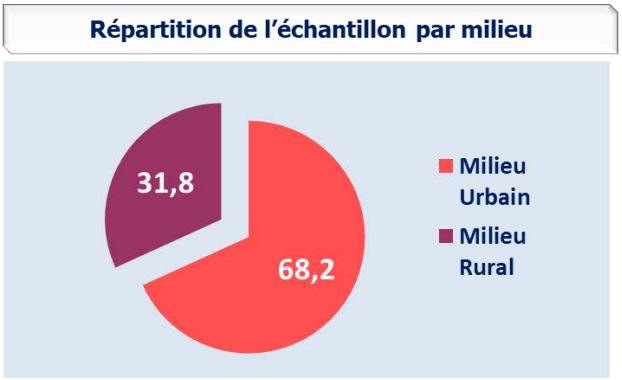
A. PREAMBULE

Afin de pouvoir déterminer la perception de la protection des données à caractère personnel au sein de la population tunisienne, une enquête a été effectuée auprès d'un échantillon de tunisiens représentatif de la population en milieu urbain et rural, composé de 1 000 Tunisiens, âgés de 18 ans et plus entre le 16 et le 23 août 2021.









Sur base des résultats, des tableaux et graphiques ont été établis et certains sont repris ci-dessous.

Pour plusieurs répondants, la protection des données personnelles est un droit de tout citoyen Tunisien. Elle permet avant tout de procurer un sentiment de sécurité aux répondants et de protéger leurs intimités.

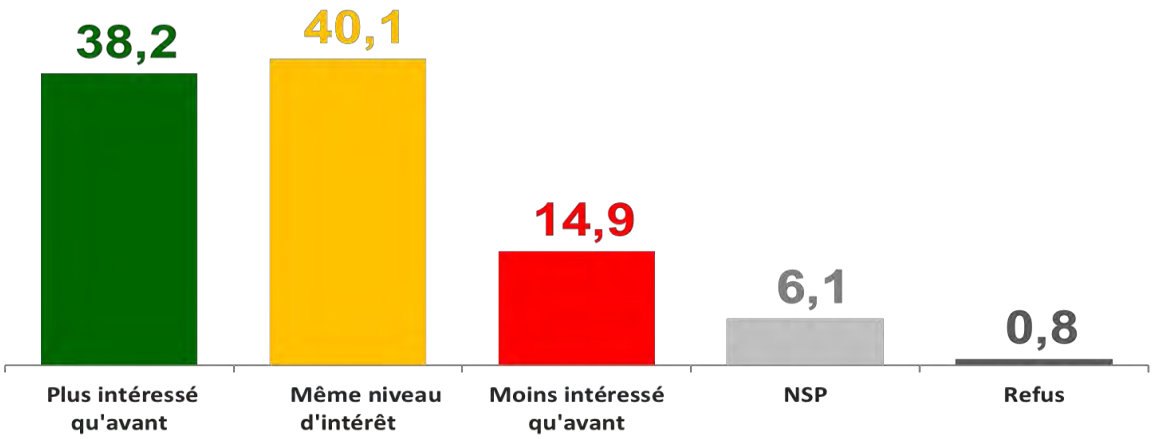
Puis par la suite, selon certains le rôle de la protection des données personnelles est de pouvoir décider quand et comment de tierces personnes peuvent utiliser ces données et à quelle fin. D'autres mentionnent la protection des données personnelles évitent le harcèlement, le chantage et les opérations de fishing.

B. RÉSULTATS DU SONDAGE DE 2021 À LA LUMIÈRE DES PRÉCÉDENTS

Pour la majorité des répondants, les données personnelles sont toutes sortes d'informations permettant d'identifier une personne, celles répétées le plus souvent sont

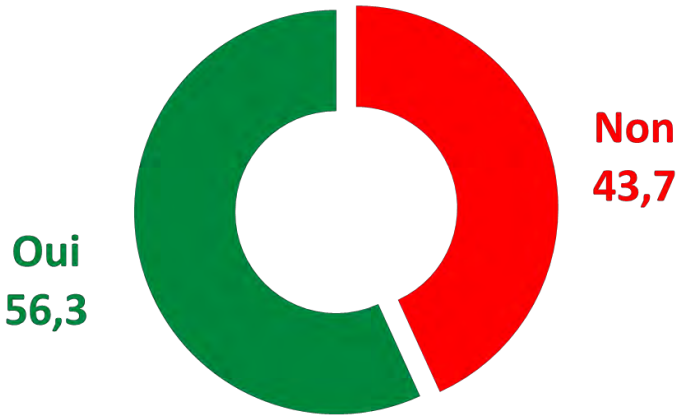
le numéro de la CIN, le nom & prénom ou encore l'adresse de résidence. Certaines personnes, principalement du secteur privé, mentionnent spontanément internet et les réseaux sociaux et leurs rôles dans la diffusion et circulation des données personnelles (photos, partages, adresses mails).

1. QUEL INTÉRÊT PORTEZ VOUS AUX DONNÉES PERSONNELLES DEPUIS LES CINQ DERNIÈRES ANNÉES ?



Nous constatons que le niveau d'intérêts est, pour 78,3% des personnes interrogées, soit équivalent soit supérieur à la situation en 2007. Cette indication est particulièrement intéressante dès lors que cela démontre que les tunisiens modifient leur approche de la protection des données à caractère personnel. Cela constitue un signal fort par rapport au pouvoir politique et devrait le convaincre le Parlement de se saisir du projet de loi de 2018 en vue de l'adopter au plus vite.

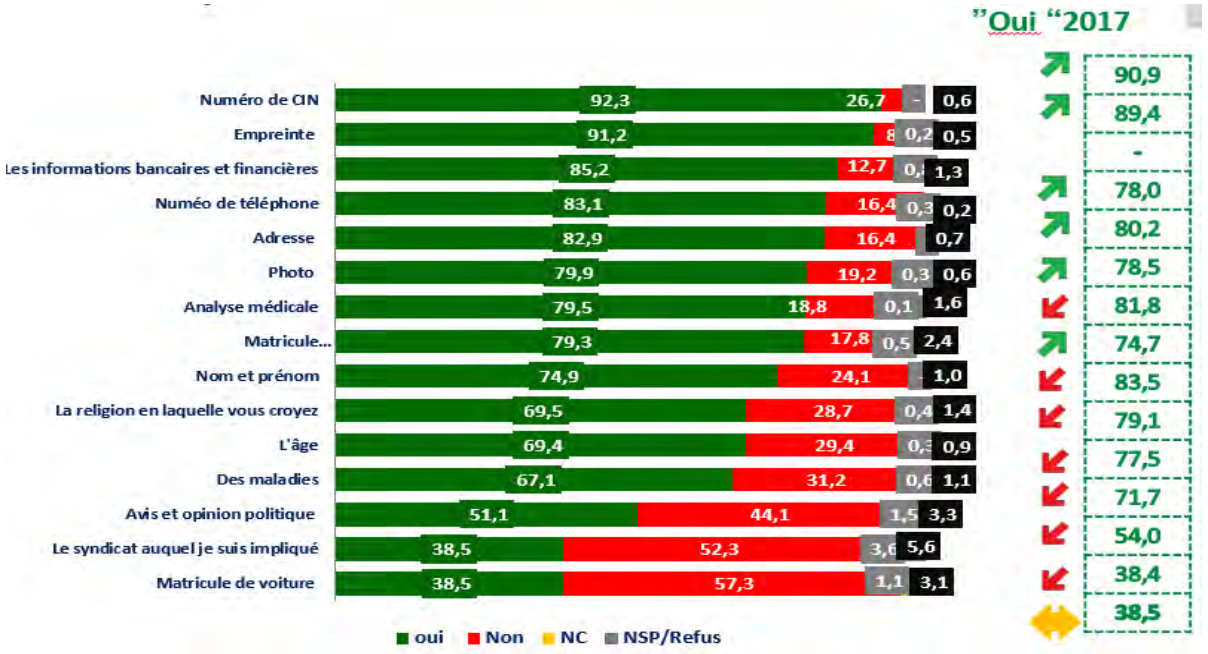
2. QUE SIGNIFIENT LES DONNÉES PERSONNELLES ?



3. QUELLES SONT LES DONNÉES PERSONNELLES ?

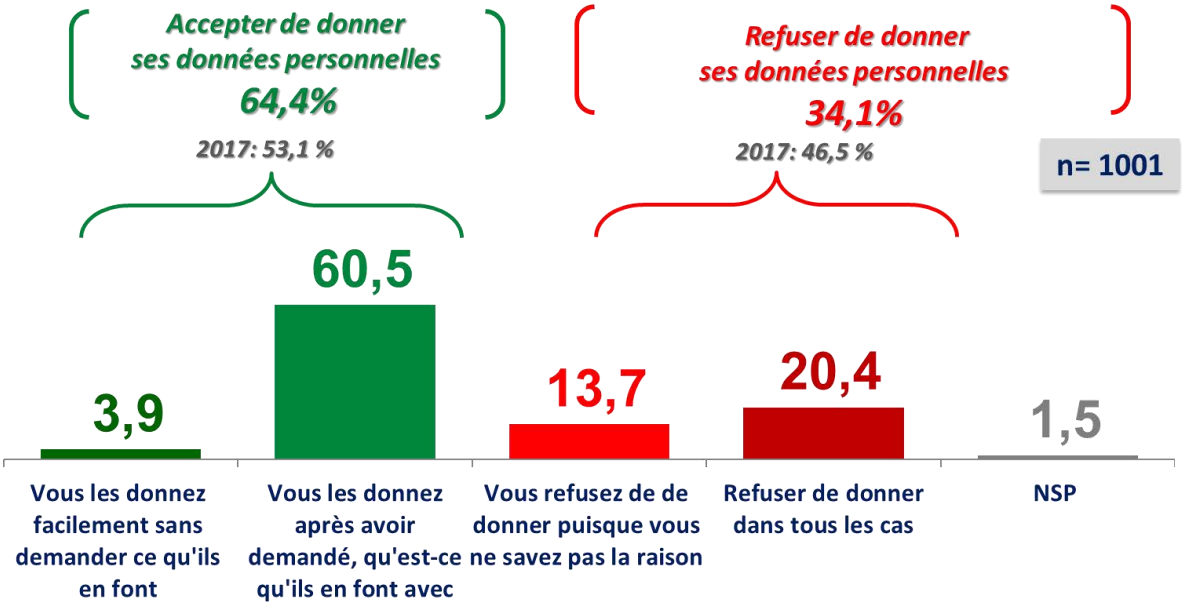
Ces résultats tendent à démontrer que, à l'instar de l'intérêt par rapport à la protection des données porté par les citoyens, ils appréhendent également mieux la notion de donnée à caractère personnel. Il n'en demeure pas moins que l'on constate, dans le graphe ci-dessus, que la notion de donnée à caractère personnel reste très cantonnée aux données évidentes alors que la notion est beaucoup plus large. La sensibilisation devrait être orientée également vers les diverses notions véhiculées par la loi sur la protection des données à caractère personnel.

4. SELON VOTRE AVIS, DITES-MOI CE QUI EST INCLUS DANS LES DONNÉES PERSONNELLES?



De manière complémentaire au point précédent, l'on constate que les éléments qui recueillent le plus de réponses positives portent sur les données habituellement catégorisées comme données à caractère personnel. Il faudrait donc que la sensibilisation qui doit être mise en place montre que la notion de "donnée à caractère personnel" est extrêmement et volontairement large.

5. EST-CE QUE VOUS PARTAGER VOS DONNÉES PERSONNELLES QUAND C'EST DEMANDÉ?



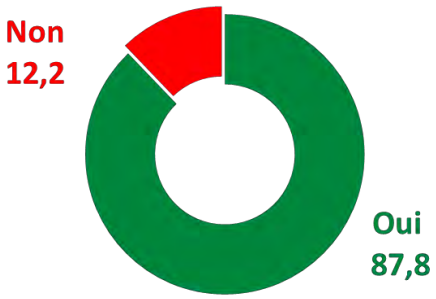
L'enquête démontre que l'intérêt que les tunisiens portent à la protection des données à caractère personnel les poussent également à analyser toute demande de partage de ces données. Nous constatons que le pourcentage de personnes interrogées acceptant de partager leurs données passent de 53,1% en 2017 à 64,4% en 2021 mais que, parmi ces 64,4%, 60,5% ne procèdent à un partage qu'après avoir demandé au demandeur ce qu'il souhaite en faire. Nous pouvons supposer qu'ils ne procèdent au partage qu'après avoir reçu une réponse rassurante sinon ils refuseraient une telle communication.

6. VOUS PENSEZ QUE VOS DONNÉES PERSONNELLES SONT UTILISÉES DANS?

La perception de l'objectif visé par l'utilisation des données à caractère personnel n'a pas réellement été modifiée durant ces 5 dernières années. Nous constatons cependant que

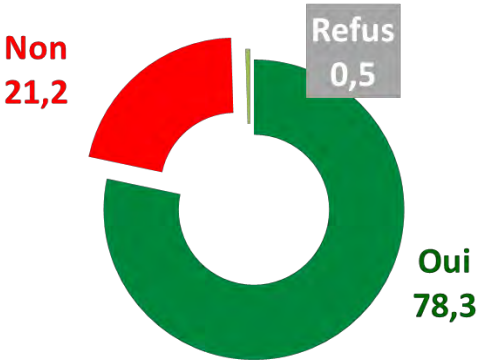
l'utilisation de nature commerciale a augmenté en termes de perception au détriment de la sécurité/surveillance et des "raisons scientifiques". Cela doit être rapproché du point 3 qui montre que les données citées comme à caractère personnel par les répondants sont celles utilisées dans le domaine commercial.

7. SAVEZ-VOUS QUE VOUS AVEZ LE DROIT DE NE PAS COMMUNIQUER TOUTES VOS DONNÉES PERSONNELLES?



Ce graphique est rassurant dès lors qu'il démontre que les citoyens savent qu'ils peuvent refuser de communiquer leurs données à caractère personnel. Ce qui est surprenant est que, quand bien même ils le savent, ils ne font pas tous application de ce choix ainsi que le montre le graphique du point 5. En effet, seuls 39% des personnes interrogées ne communiquent leurs données qu'après avoir demandé au demandeur ce qu'il souhaite en faire

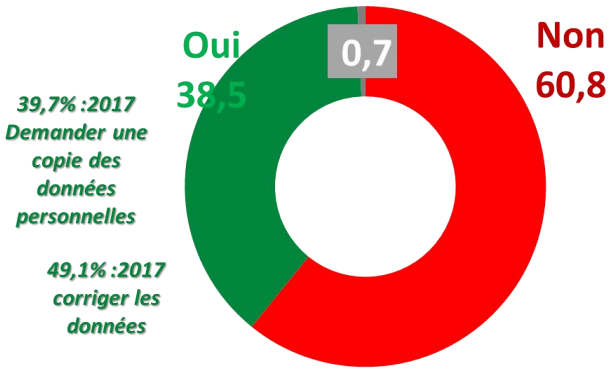
8. QUAND VOUS ÊTES EMMENÉ À COMMUNIQUER VOS DONNÉES PERSONNELLES, CONSULTEZ-VOUS LES CONDITIONS GÉNÉRALES ?



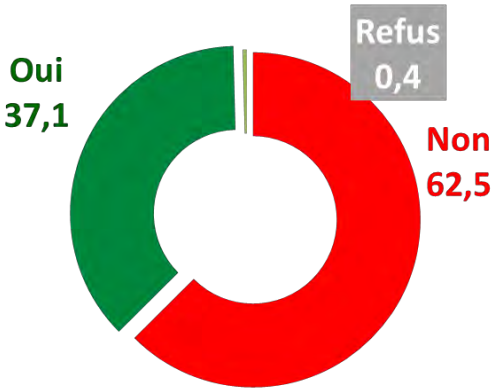
En 2017, 78,4% des personnes interrogées avaient répondu qu'elles lisaient les conditions générales avant tout achat. Le pourcentage reste donc stable alors que, d'autre part, l'intérêt des tunisiens à l'égard de la protection des données à caractère personnel a fortement augmenté.

9. LES DROITS DE LA PERSONNE CONCERNÉE

Savez-vous que vous avez le droit de demander une copie de vos données personnelles que vous leur avez fournies, et vous avez le droit de demander qu'elles soient corrigées.

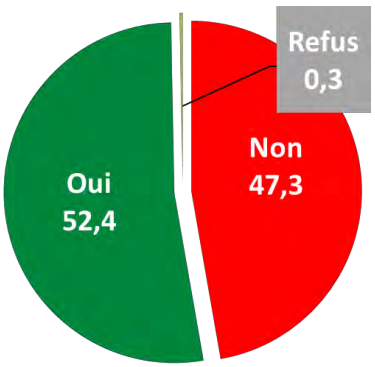


Avez-vous déjà demandé une copie des conditions d'utilisation pour les lire et qui peut vous amenez à retirer votre approbation ?



Ces deux graphiques sont inquiétants dès lors qu'ils démontrent que les citoyens n'ont pas conscience des droits que la loi sur la protection des données à caractère personnel leur octroie. En effet, le consentement, les droits d'accès (et de copie) et de modification sont essentiels en matière de protection des données. Or, ils paraissent très méconnus alors que, par ailleurs, une majorité de répondants affirment lire les conditions générales. Cela démontre qu'une réelle campagne de sensibilisation doit être effectuée afin que les citoyens soient avertis de leurs droits et soient en mesure de les exercer !

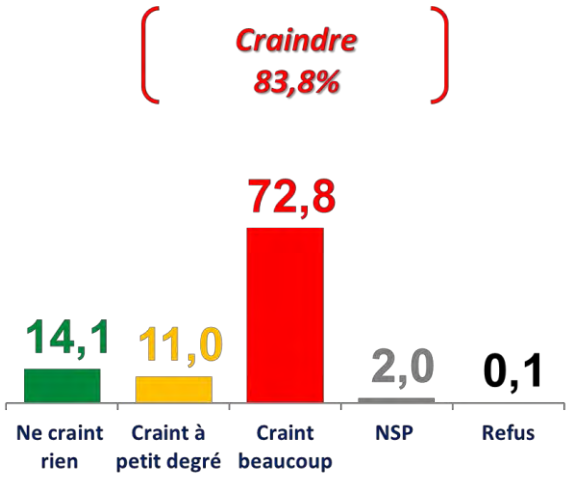
10. Vous savez que quand vous donnez vos données personnelles à d'autres personnes, ils peuvent être envoyés même à l'étranger ?



Même si le pourcentage de "oui" est légèrement supérieur à celui du "non", ce graphique montre, d'une part, la méconnaissance des citoyens par rapport à l'utilisation qui est faite

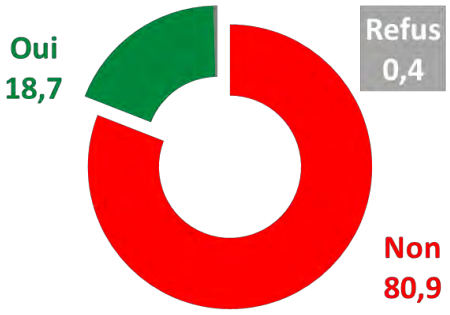
des données qui les concernent mais également, d'autre part, les lacunes dans l'information qui est délivrée par les responsables du traitement. Une sensibilisation doit donc être mise en place à deux niveaux : celui des responsables du traitement et celui des personnes concernées.

11. A QUEL NIVEAU VOUS CRAIGNEZ QUE VOS DONNÉES PERSONNELLES SOIENT TRANSMISES À D'AUTRES PERSONNES, MÊME À L'ÉTRANGER ?



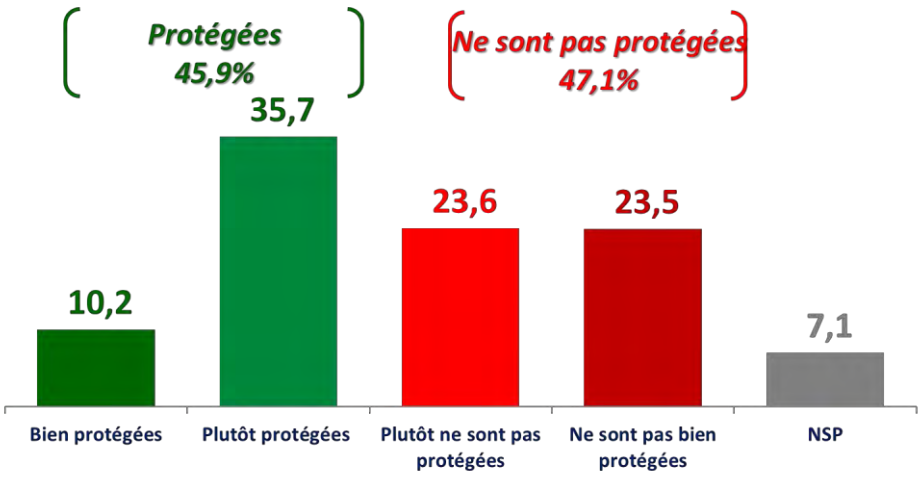
Ce graphique démontre que les citoyens ont une réelle crainte dans le sort réservé à leurs données qui est couplée au fait qu'ils ne connaissent pas leurs droits issus de la loi sur la protection des données. A nouveau, un travail de sensibilisation est urgent et doit être effectué de manière transversale afin de toucher tant les citoyens que les responsables du traitement des secteurs public et privé.

12. VOUS ESTIMEZ QUE LA RÉPONSE NÉGATIVE À UN SERVICE QUE VOUS DEMANDEZ À DES STRUCTURES PRIVÉES SE BASE SUR LES DONNÉES PERSONNELLES QU'ILS ONT CONNAISSANCE DE VOUS ?



Si les citoyens craignent de manière importante un transfert des données à caractère personnel les concernant vers des tiers, ils considèrent que les entreprises du secteur privé n'abusent cependant pas de leur droit dès lors qu'ils n'ont pas l'impression que ces entreprises prennent des décisions sur base d'une analyse des données à caractère personnel qu'elles auraient sur leurs clients. Cela peut paraître paradoxal.

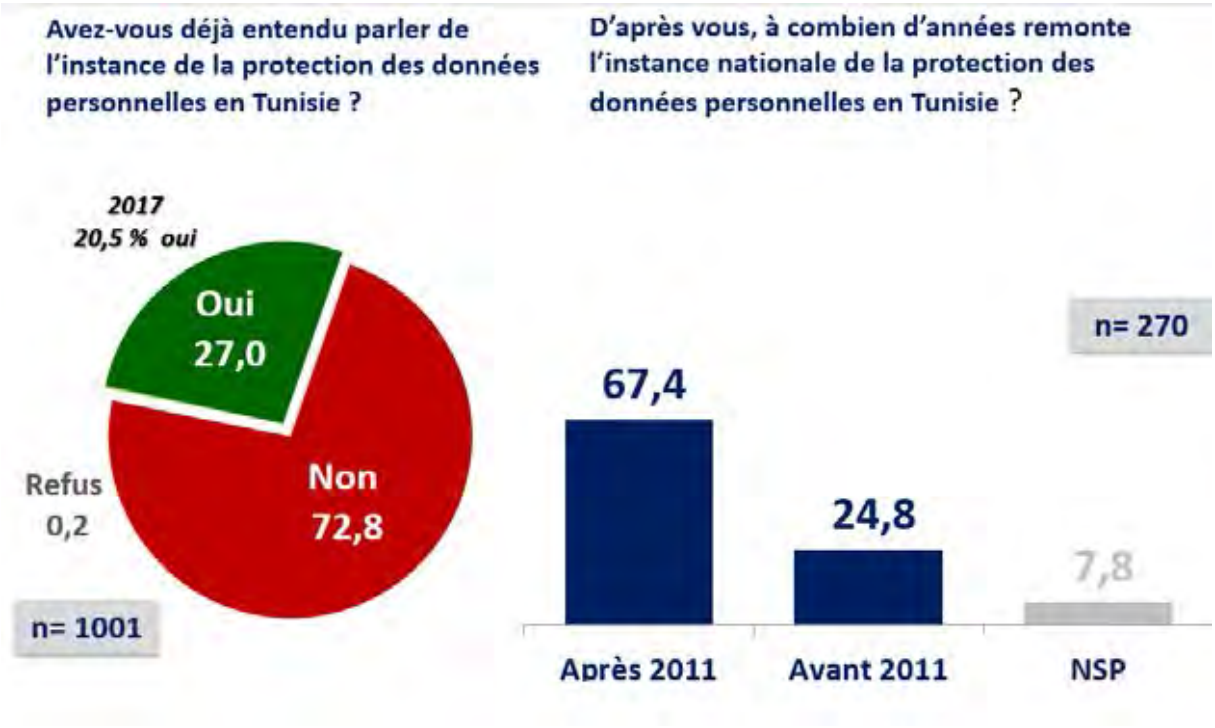
13. A QUEL DEGRÉ PENSEZ-VOUS QUE LES DONNÉES PERSONNELLES SONT PROTÉGÉES ?



Ce graphique semble être complémentaire à celui repris au point 11. Il y a manifestement une crainte parmi les citoyens qui se porte tant sur l'usage des données mais également la sécurité qui entoure leur traitement.

Que cette crainte soit fondée ou pas, cela doit inciter l'Instance à mettre en place un réel programme de contrôle des responsables du traitement afin de vérifier que les mesures de sécurité sont conformes aux règles de l'art en la matière.

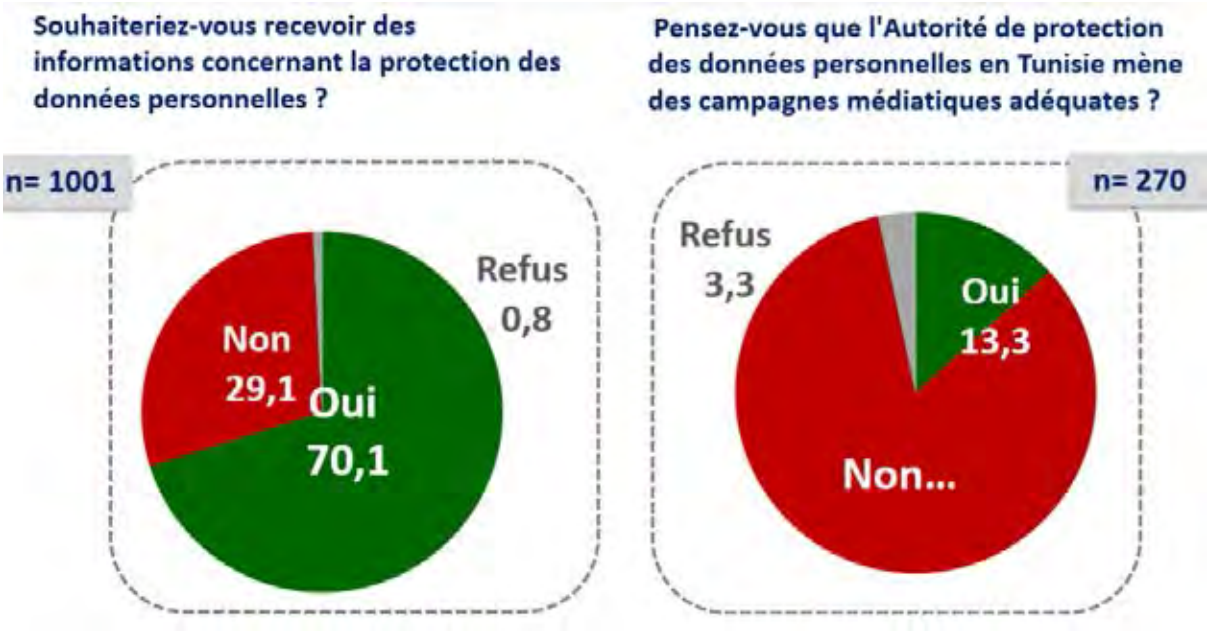
14. L'INSTANCE DE LA PROTECTION DES DONNÉES PERSONNELLES EN TUNISIE



Manifestement, les citoyens interrogés ne connaissent pas l'existence de l'Instance, ce qui est inquiétant mais pas surprenant. En effet, plusieurs graphiques montrent, ainsi que nous l'avons déjà relevé, que les citoyens ne sont pas conscients de leurs droits et le fait de ne pas connaître l'existence de l'Instance y est très lié.

Cela montre une méconnaissance de la loi elle-même qui doit faire l'objet de publications, de campagne de sensibilisation et surtout de vulgarisation. Il s'agit d'un travail urgent. Et cela l'est

d'autant plus que les citoyens sont en demande et qu'ils sont une toute grand majorité de considérer que l'Instance ne mène pas des campagnes médiatiques adéquates.



VI. Recommandations

Il ne fait aucun doute que la protection des données est devenue un droit fondamental en soi, même s'il est intimement lié à la protection de la vie privée qui a cependant une portée plus large.

Au titre de liberté fondamentale, il doit avoir une législation forte mais également une législation visible et connue tant des citoyens que des acteurs publics et privés.

Si la Tunisie l'a, dès 2002, inscrite comme norme constitutionnelle pour ensuite adopter la loi organique n° 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel rendant ainsi la Tunisie précurseur dans la région, il n'en demeure pas moins que la sensibilisation doit être mise en place. Elle permettra aux divers acteurs, y compris les citoyens, de "s'approprier" la loi. L'enquête reprise en partie ci-dessus démontre que le citoyen craint la mauvaise utilisation qui peut être faite sur les données à caractère personnel le concernant et n'a pas connaissance des droits qui sont les siens en termes de protection des données à caractère personnel. Les responsables du traitement et les sous-traitants, qu'ils soient du secteur public ou privé, devraient être sensibilisés et par la suite sanctionner de manière sévère les éventuelles infractions à la loi dès lors que le contrevenant ne pourra plus se retrancher derrière une hypothétique méconnaissance de la législation.

Pour rehausser le niveau de la culture en matière de protection des données personnelles et assurer une effective application de la loi, des recommandations sont présentés à la fin de ce livre blanc :

1. L'ÉDUCATION À LA PROTECTION DES DONNÉES

La seule manière de réaliser cet objectif est de se livrer à un programme d'insertion de la protection des données personnelles dans le cursus d'enseignement. Si dans les petites classes et avec les jeunes il serait utile et même nécessaire de sensibiliser à un meilleur comportement de tous les jours en relation avec la préservation de sa vie privée et de la protection des données personnelles : Comment naviguer sur Internet ? Comment utiliser de manière responsable les réseaux sociaux ? Comment évaluer le comportement des personnes en relation avec leurs données personnelles ? Les réponses à ces questionnements doivent venir de supports non intrusifs loin des programmes officiels des enseignements déjà surchargés. Des planches graphiques à placarder sur les murs des classes d'enseignement donneraient plus d'effet à cette action.

A un autre niveau et à partir de l'Université, les spécialités qui donneront lieu à des professions en relation avec la protection des données personnelles doivent voir la question incluse dans leur programme d'enseignement. Est-ce normal qu'un médecin ou un juge tout au long de sa formation n'a jamais eu une heure d'enseignement sur la protection des données personnelles ? Les cursus juridiques mais aussi informatiques ainsi que tous ceux en relation avec la santé ou les médias doivent voir inclure un nombre d'heures réservés à ce domaine important pour l'exercice idoine par la suite de la profession à laquelle ils sont destinés.

Au niveau de la justice elle-même, il conviendrait de procéder à la formation de magistrats à la protection des données à caractère personnel afin qu'ils puissent avoir les connaissances suffisantes pour traiter les dossiers liés à cette matière. L'on pourrait imaginer aussi la création de chambres spécialisées en protection des données à caractère personnel ou des magistrats référents connus de leurs collègues qui leur serviraient de recours pour mieux traiter les dossiers qui leur sont soumis en relation avec la protection des données personnelles.

C'est aussi le cas en ce qui concerne l'Ecole Nationale d'Administration qui forme les futurs cadres et gestionnaires de la fonction publique et les décideurs de l'Etat. Il est donc important que la question de la protection des données personnelles soit introduite dans le cursus de formation et qui permettrait de sensibiliser sur l'importance de la mise en place d'un régime de protection et de travailler à son effectivité dans le secteur public qui peut servir de best practice.

Dans ce cadre général relatif à l'éducation et à l'enseignement, les formateurs doivent être dotées d'un outil de travail car ils sont eux même le produit du système lacunaire de formation dans le domaine de la protection des données personnelles. Une boite à outil permettrait de leur indiquer les axes importants sur lesquels ils devraient axer leur sensibilisation et formation des apprenants. Mais aussi un tel support mettra à leur disposition des outils didactiques qu'ils pourront utiliser dans cette mission.

2. SENSIBILISATION À LA PROTECTION DES DONNÉES

Une des actions prioritaire est d'installer la culture de la protection des données personnelles dans la société tunisienne. C'est d'ailleurs la mission la plus importante de l'Instance de protection. La protection des données personnelles est une nouveauté qui s'impose et qui s'impose comme un impératif devant la digitalisation flagrante et l'utilisation parfois exagérée des citoyens des technologies de communication modernes très intrusives pour les données personnelles.

L'Instance est à côté de l'enseignement et de l'éducation les structures dont la mission est importante pour installer la culture de la protection à travers la sensibilisation des individus à la protection des données personnelles.

Pour ce faire, il faut nécessairement que l'Instance dispose des moyens nécessaires en termes tant de ressource humaine que financiers pour mener à bien ses missions qui sont nombreuses. Pour remplir les conditions standards d'une autorité indépendante, il est nécessaire de prévoir des moyens pérennes. Il faut également que ces moyens lui permettent de faire connaitre ses actions auprès des citoyens.

Cette visibilité peut prendre diverses formes telles que des capsules de sensibilisation, une formation en ligne à l'image des MOOC plus facilement accessibles, des référentiels dans les différents domaines relatifs à la protection des données personnelles, mais aussi susciter des décisions de justice traitant de la protection des données et appliquant les normes légales dans le domaine.

3. CONTRÔLE & ACCOMPAGNEMENT DANS LA PROTECTION DES DONNÉES

L'Instance nationale de protection a pour mission de faire évoluer la culture de la protection sur le territoire national, mais d'un autre côté elle est chargée d'une autre mission, celle de contrôler la conformité des traitements des données personnelles aux normes de protection. Comme toutes les instances similaires sur le plan international, c'est une instance de contrôle. Car aucune norme ne se justifie si on ne met pas en place une structure dédiée pour s'assurer du respect des règles établies.

Le contrôle est la mission la plus ardue, car elle ne peut être efficace et percutante que si les structures qui s'en chargent sont dotées des moyens leur permettant de mener à bien cette tâche et le professionnalisme nécessaire. Parmi les missions des instances, le contrôle est celle qui demande le plus d'implication et de moyens humains.

Mais les instances de contrôle ont dans ce cadre une autre mission, celle d'accompagner les responsables de traitement dans leur action de mise en conformité. Dans un espace où la culture ne s'est pas développée dans ce domaine et que les institutions de formation n'incluent pas cette problématique dans leur cursus, la société nationale reste dépourvue d'experts dans le domaine. L'Instance de contrôle devient le seul recours des responsables de traitement pour amorcer et aller de l'avant dans leur projet de mise en conformité.

L'Instance ne peut assurer ces missions importante de contrôle des activités de traitement des données personnelles, d'accompagnement des responsables de traitement dans leur mise en conformité et entre autres de réponse aux demandes d'avis, si elle n'est pas dotée de moyens humains qualifié. L'Instance nationale en est actuellement dépourvue.

4. ADOPTER UN NOUVEAU CADRE JURIDIQUE

Le cadre juridique tunisien dans ce domaine souffre de plusieurs lacunes et principalement une loi qui date de 2004 édictée par un régime loin d'être préoccupé par le consécration des droits humains et qui depuis n'a jamais été révisé pour s'adapter à l'évolution des méthodes de traitement des données.

La Tunisie a fait évoluer son cadre juridique en adhérant à la convention 108 du Conseil de l'Europe en 2017 qui a conformément à l'article 20 de la constitution révisé implicitement la loi organique de 2004 en abrogeant plusieurs disposition et principalement les articles 16 et 53 et 54 qui instituent des régimes d'exceptions injustifiés et exagérés au profit des personnes publiques et des employeurs.

C'est dans ce cadre que la Tunisie a élaboré un nouveau projet de loi qui essaye de se rapprocher des meilleurs normes actuellement en vigueur dans le monde à l'image de celles consacrées dans le Règlement Général de la Protection des Données personnel européen (RGPD). Le projet a été transmis en mars 2018 au Parlement et depuis est sur le bureau de la commission des droits et des libertés.

En 2019, la Tunisie a procédé à la signature du protocole additionnel de la convention 108 qui la modernise et la met au niveau de la protection instauré par le RGPD. Mais la Tunisie ne pourra ratifier le protocole additionnel et s'y soumettre que si la nouvelle loi nationale est adoptée ou tout au moins réviser la loi organique de 2004.

A défaut de nouvelle loi, il est impératif de réviser en attendant celle de 2004 à travers un projet touchant au maximum une quinzaine d'articles qui font évoluer le statut de l'Instance de contrôle et ses pouvoirs , en introduisant des mises en conformité avec les normes comparées en créant la fonction de délégué à la protection des données personnelles mais aussi en abrogeant le régime spécifique de dispense trop large au profit des personnes publiques.

Cette mise à niveau du cadre national permettra de rehausser le niveau de protection en donnant plus d'indépendance et de pouvoirs à l'Instance de protection. L'amélioration de la protection en Tunisie lui permettra d'aspirer à l'adéquation européenne qui ouvrira la voie à plus d'échange de données personnelles avec l'espace européen.

Une législation répondant aux standards de protection des données à caractère personnel permettra également d'envisager une éventuelle demande de décision d'adéquation auprès de l'Union européenne avec laquelle les entreprises tunisiennes ont de nombreuses relations commerciales. Si cet objectif peut paraître ambitieux, il faut y tendre et mettre en œuvre les moyens nécessaires à assurer une réelle effectivité de la loi sur la protection des données à caractère personnel.