CIBA Conférence Information Bibliothèques Archives

2ème édition | 26-28 août 2022 |

Evénement virtuel

Gouvernance de l'information et du numérique

Communication

# Les enjeux de la protection des données personnelles à l'ère de l'administration électronique

Hector Houétchénou Ahogni
Enabel, Cotonou, Bénin

Wenceslas Mahoussi
Edubourses, Abomey-Calavi, Bénin

&

Prudence Kouchade
Edubourses, Abomey-Calavi, Bénin

Hector Ahogni est titulaire d'une Licence professionnelle en Administration du Travail et Sécurité Sociale et d'un Master professionnel en Management des Services Publics obtenus respectivement en 2008 et en 2019 à l'École nationale d'Administration (Université d'Abomey-Calavi). Il a été le Chef de la cellule de contrôle des marchés publics et assistant du Secrétaire général de l'Autorité de Protection des Données Personnelles. Il peut être joint à l'adresse hectorahogni@gmail.com.

Wenceslas Mahoussi est titulaire d'un doctorat en Sciences de l'Information et de la Communication. Inscrit sur la liste d'aptitude aux fonctions de Maître-Assistant du Conseil Africain et Malgache pour l'Enseignement Supérieur en juillet 2022, il est enseignant à l'Université d'Abomey-Calavi. Il peut être joint à l'adresse wenceslas.mahoussi@uac.bj.

Prudence Kouchade est titulaire d'une Licence professionnelle en Archivistique obtenue en 2021 à l'Ecole nationale d'Administration (Université d'Abomey-Calavi). Il est assistant de recherche à l'Observatoire des Sciences de l'Information et de la Communication de EDUBOURSES. Il peut être joint à l'adresse prudencekouchade@gmail.com.

# Les enjeux de la protection des données personnelles à l'ère de l'administration électronique u Bénin

Hector Houétchénou Ahogni
*Enabel, Cotonou, Bénin*

Wenceslas Mahoussi
*Edubourses, Abomey-Calavi, Bénin*

Prudence Kouchade
*Edubourses, Abomey-Calavi, Bénin*

**Résumé**

L'essor des technologies numériques a généré une permanence connexion de la société au cyberespace. Dans cette dynamique, nous assistons à la naissance aujourd'hui d'une notion capitale : il s'agit de la traçabilité dans les systèmes d'information. Elle s'est progressivement conjuguée aux pratiques d'identification et de suivi des personnes ; ces dernières sont décrites par des « données » de natures diverses. Indissociables des TIC, les enjeux résident désormais dans les modes de protection des données personnelles mis en œuvre dans les sociétés aux fins de e-marketing, de nouveaux modèles économiques pour les uns et la sécurité des États pour les autres. Elles se matérialisent alors dans un ensemble de textes, de techniques, d'acteurs, de politiques et de pratiques en interrelation. Dès lors, avec le numérique, les données personnelles deviennent omniprésentes et posent le problème de la nécessité de protection de la vie privée des usagers sur internet, une préoccupation majeure des sociétés et des États, puisque les sites web, les réseaux sociaux et applications mobiles incitent les internautes à dévoiler leur vie privée. Les TIC ont ainsi multiplié les possibilités de collecte et de traitement des données, en particulier celles à caractère personnel. Aussi, l'explosion des médias sociaux, les moyens de géolocalisation et de vidéosurveillance, le développement de la biométrie ont pour conséquence l'accroissement des risques d'atteintes aux libertés publiques et à la vie privée.

**Mots clés** : *Données personnelles –Numérique– Cyberespace - Cybersécurité - Bénin*

## Introduction

La « révolution numérique » a fait son entrée dans les sociétés de consommation dans les années 1960 avec la messagerie instantanée et le courrier électronique. C'est surtout entre 1980 et 2000, grâce à l'industrialisation des processeurs et de l'ordinateur, qu'une « révolution numérique » se produit embrassant tous les secteurs d'activités, les produits et services. Dès lors, l'accès à internet sur

téléphone, l'apparition de la 4G1 et de la 5G2, la progression des objets connectés, la multiplicité des applications et médias sociaux, des blogs et vidéos démontrent l'hyper-connexion des sociétés transformant le monde en un village planétaire. Toutefois, avec le numérique, les données personnelles deviennent omniprésentes et posent le problème de la nécessité de protection de la vie privée des usagers sur internet qui constitue une préoccupation majeure des sociétés et des États sous prétexte d'un contrôle inexistant quant à la protection de l'intégrité physique et intellectuelle humaine. Les TIC ont ainsi multiplié les possibilités de collecte et de traitement des données personnelles amplifiant ainsi les risques d'atteintes aux libertés publiques et à la vie privée.

Face à cette situation, la protection de la vie privée et des données à caractère personnel est devenue un défi majeur tant pour les entreprises, les autorités que pour les consommateurs. Dans une société où les données personnelles sont de plus en plus considérées comme un moyen de paiement et où réseaux sociaux (Facebook, Twitter, LinkedIn, YouTube, etc.) sont devenus les principaux canaux indispensables à toute diffusion informationnelle, la vie privée des usagers est de plus en plus menacée. Une protection juridique basée sur la création d'un texte législatif et d'un organe de régulation et de contrôle est donc l'approche indispensable pour canaliser les agissements des uns et des autres dans cet environnement rempli d'incompréhension et d'immaturité. Quel est l'encadrement juridique de la protection des données personnelles au Bénin ? Quels sont les usages et les mécanismes de protection des données personnelles au Bénin ? Quels comportements et outils les personnes, entreprises et l'administration étatiques doivent-elles mettre en place face à la recrudescence de la cybercriminalité et l'insécurité du fait de la manipulation des données personnelles à l'ère de l'économie numérique ?

Ces préoccupations suscitent des réflexions profondes qui seront menées tout au long de notre étude. Elle est structurée en trois parties : les principes fondamentaux de la protection des données personnelles ; les limites à une protection optimale desdites donnée et les recommandations pour une gestion rassurante et sécurisante des données personnelles et de la vie privée.

## Les principes fondamentaux de la protection des données personnelles

Les principes de la protection des données personnelles sont élaborés dans le souci de protéger l'individu d'un usage pervers ou déviant de ses données dans le cyberespace. Nous explorerons d'abord les obligations des responsables de

[1] 4ème génération de la technologie de téléphonie mobile à haut débit de connexion internet.

[2] 5ème génération de la technologie de téléphonie mobile à très haut débit de connexion internet.

traitements, les droits des personnes dont les données sont traitées, ensuite nous verrons les formalités préalables à un traitement et les dérogations possibles.

### *Les obligations du responsable de traitement*

Le responsable du traitement est astreint sous peine de sanction, au respect des principes ci-après :

### *L'analyse d'impact de traitement avant la mise en œuvre de certains traitements*

Lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, une analyse d'impact sur la protection des données doit être menée.[3]

### *Le respect du principe de licéité en matière de collecte des données*

Selon ce principe, les données doivent être collectées de manière loyale, c'est-à-dire que la personne concernée doit être consciente que ses données font l'objet d'une collecte et doit pouvoir s'y opposer. Elles doivent être collectées de manière licite, les moyens mis en œuvre pour collecter les informations devant être légaux.

### *Le respect du principe de la finalité*

La finalité, c'est l'objectif principal qui a guidé la mise œuvre du traitement. Les informations qui concernent les personnes ne peuvent être recueillies et traitées que pour un usage déterminé et légitime. Les données ne doivent donc plus être utilisées de manière incompatible avec l'objectif déclaré.

### *Le principe du consentement et de légitimité*

Les données à caractère personnel (DCP) doivent être obtenues et traitées loyalement et licitement. Le traitement des DCP est considéré comme légitime si la personne dont on collecte et traite les données donne son consentement préalable par écrit, sauf si la loi autorise à le faire sans son consentement.

### *L'obligation de sécurité*

Le responsable de traitement doit garantir la disponibilité, l'authenticité, l'intégrité et la confidentialité des données contre toute atteinte accidentelle (désastres naturels, incidents techniques, etc.) ou volontaire. Il doit ainsi prendre « toutes précautions utiles afin de préserver la sécurité des informations ».

[3] Article 428 du code du numérique

### *Le principe d'une durée limitée de conservation*

Les informations ne peuvent être conservées pour une durée illimitée. Elles doivent être conservées pendant une durée n'excédant pas celle nécessaire à l'atteinte des finalités pour lesquelles elles sont enregistrées. Sauf en cas d'autorisation spéciale de l'APDP, la durée de conservation peut être déterminée en fonction de la finalité de chaque fichier.

### *Le principe de la proportionnalité*

En vertu de ce principe, les données doivent être adéquates, pertinentes, exactes et non excessives par rapport aux finalités pour lesquelles elles sont collectées.

### *Le principe de confidentialité*

Tout responsable de traitement doit prendre les mesures nécessaires pour garantir la confidentialité des informations et éviter leur divulgation à des tiers non autorisés. Le responsable du traitement doit veiller à ce que toute forme de manipulation ou de consultation soit exclusivement effectuée par des personnes habilitées qui agissent sous son autorité et sur ses instructions.

### *Tenue d'un registre des activités liées au traitement*

Chaque responsable du traitement ou son représentant tient un registre des activités de traitements effectués. Ce registre doit comporter toutes les informations énumérées à l'art. 435 du code du numérique.

### *L'établissement d'un rapport annuel à transmettre à l'APDP*

Le responsable du traitement est tenu d'établir un rapport annuel pour rendre compte à l'APDP de ses activités.

### *La désignation d'un délégué à la protection des données à caractère personnel*

Une autre innovation du code du numérique relativement à la protection des données personnelles est la désignation de délégué à la protection des données personnelles au sein des entreprises ou sociétés (privées et publiques).

## Les droits de la personne concernée par un traitement

### *Le droit d'accès*

Ce droit postule que les personnes concernées ont le droit de connaître les données conservées et traitées qui les concernent auprès de toute personne ou

organisme responsable de traitement. Ce droit peut s'exercer par l'accès direct ou indirect.

### *Le droit de rectification et de suppression*

La personne dont les données sont collectées peut exiger du responsable la correction, la mise à jour, ou la suppression des données personnelles la concernant et qui sont inexactes, incomplètes, équivoques, périmées ou même celles dont la collecte, l'utilisation, la communication et la conservation sont interdites par la loi[4].

En 2011, Max Schrems, étudiant autrichien, s'est adressé à Facebook afin d'obtenir communication de l'ensemble de ses données détenues par ce dernier. Il a ainsi reçu, quelques semaines plus tard, communication de 1 222 pages en format PDF. Choqué par le volume d'informations conservées (qui comprenaient également des données qu'il avait pu effacer dans le passé), il a décidé de porter plainte et il a créé une association nommée Europe-v- Facebook qui rassemble aujourd'hui plus de 25 000 plaignants.

### *Le droit d'opposition*

Toute personne concernée peut, pour des raisons légitimes (risque d'atteinte à sa vie privée, manque de confidentialité, risque de divulgation), s'opposer à ce que des données la concernant fassent l'objet de manipulation, sauf si le traitement de données présente un caractère obligatoire. Dans le cadre des traitements à des fins de police judiciaire, ces droits sont soumis à des restrictions. Mais la loi reconnait également un certain nombre de principes et impose des obligations au responsable de traitement.

### *Le droit à l'oubli*

Il s'agit d'une obligation à la charge du responsable du traitement consistant à faire cesser la diffusion des données d'un individu notamment si la personne concernée ne consent plus à leurs utilisations[5].

Le droit à l'oubli n'est qu'une facette du droit à l'effacement, et concerne en somme une « fin de vie » des données. Les données stockées doivent en effet être soumises à une durée de conservation, bien définie au moment où le stockage

[4] Article 441 du code du numérique

[5] Article 443 du code du numérique

commence. Cette durée doit être précisée à la personne concernée lors du recueil du consentement, si celui-ci est requis[6].

L'une des questions qui se pose sur la problématique du droit à l'oubli est de savoir comment sont mémorisées les condamnations et comment conjuguer l'injonction du droit à l'oubli avec le déploiement des nouvelles technologies et la mise en place de fichiers pour conserver les condamnations.[7]

### *Le droit à la portabilité des données*

Conformément aux dispositions de l'article 438 du code du numérique « *les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* ».

En somme, les données à caractère personnel faisant l'objet d'une demande de portabilité doivent pouvoir être réutilisées par le destinataire, à savoir le nouveau responsable du traitement ou la personne concernée elle-même.

Au Bénin le droit à la portabilité est une effectivité dans le secteur de la téléphonie mobile où un abonné peut changer d'opérateur GSM sans changer son numéro de téléphone après trois mois d'utilisation continue.

La question que l'on est en droit de se poser est de savoir si la portabilité entraine l'inexploitation ou la suppression des données de l'abonné par l'opérateur initial.

Le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant

Excepté les cas de dérogations légales, toute personne concernée par un traitement a droit à un recours juridictionnel effectif si elle considère que les droits que lui confèrent les dispositions du livre cinquième du code du numérique ont été violés du fait de ce traitement de ses données à caractère personnel effectué en violation des dispositions dudit livre.

[6] Le RGPD : nouveau droit de la protection des données personnelles, TALONE, 2019

[7] http://www.justice.gouv.fr/justice-penale-11330/le-sens-de-la-peine-et-le-droit-a-loubli--28524.html

*Le droit à réparation et responsabilité*

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation des dispositions du Livre V a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Certains traitements de données à caractère personnel sont dérogés des formalités préalables, d'autres obéissent à des mesures spécifiques.

Les dérogations et les mesures spécifiques liées aux transferts de données personnelles

Les mesures spécifiques liées aux transferts : On entend par transfert de données personnelles : « *toute communication, toute copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, toute copie ou déplacement de ces données d'un support à un autre, quel que soit ce support dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire* ».

Au Bénin le transfert obéit à des règles générales et à des exceptions[8].

Règles générales

Le transfert des données à caractère personnel vers un État tiers ou une Organisation Internationale ne peut avoir lieu que, lorsque l'Autorité constate que l'État ou l'Organisation Internationale en question assure un niveau de protection équivalent à celui mis en place par les dispositions du Livre portant protection des données personnelles. Par conséquent, avant tout transfert de données à caractère personnel vers un État tiers ou une Organisation Internationale, le responsable du traitement doit préalablement obtenir l'autorisation de l'Autorité.

Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données. Le caractère équivalent et suffisant est déterminé en tenant compte de critères comme l'État de droit, le respect des droits de l'homme et des libertés fondamentales, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer.

[8] Article 391 du code du numérique

*Les exceptions en matière de transfert*

« Un transfert ou une catégorie de transferts de données à caractère personnel vers un État tiers ou une Organisation Internationale n'assurant pas un niveau de protection adéquat, peut être effectué dans un des cas suivants :

i) la personne concernée a expressément donné son consentement au transfert envisagé ;
ii) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée ;
iii) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;
iv) le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;
le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;
v) le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

## *Les limites à une protection optimale des données personnelles dans un contexte de généralisation de l'utilisation des données personnelles*

### Les limites liées aux imperfections du code du numérique

### Quelques dispositions à polémiques

Un avis de l'APDP dans le cas des traitements opérés pour le compte de l'État

Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont autorisés par décret pris en Conseil des ministres après avis motivé de l'Autorité[9]. Ces traitements portent sur :

i) la sûreté de l'État, la défense ou la sécurité publique ;

[9] Article 411 du code du numérique

ii) la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
iii) le recensement de la population ;
iv) les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;
v) le traitement de salaires, pensions, impôts, taxes et autres liquidations.

L'avis de l'Autorité est publié avec le décret autorisant ou refusant le traitement.
Cette disposition fragilise quelque peu la puissance de l'APDP dans son rôle de veille et de garant de protection des données personnelles et de la vie privée au Bénin. En effet, lorsque le pouvoir exécutif initie un traitement qui est rangé dans l'un des cinq points ci-dessus, il n'est requis qu'un avis consultatif de l'Autorité. Il est donc loisible au gouvernement de rendre exécutoire un traitement qui viole un droit fondamental par la prise d'un décret en Conseil des Ministres autorisant ledit traitement.

### *Principe de responsabilité des responsables de traitement*

Le législateur à travers le livre Vème du code du numérique n'impose plus au responsable de traitement l'obligation de déclaration des traitements de données personnelles opérées auprès de l'Autorité (article 405 du code du numérique). Il a pris des mesures (tenue de registres de traitement de données, désignation des délégués à la protection des données personnelles, rapport annuel sur les activités de traitement de données personnelles à adresser à l'Autorité…) qui établissent l'Autorité au rang de « Contrôleur » des activités de traitement de données personnelles.

Cette position du législateur pose un problème d'application étant donné qu'au Bénin la protection des données personnelles et le respect de la vie privée sont des concepts nouveaux et l'expérience en est encore à l'étape embryonnaire. Les années d'expérience qui ont permis à l'Union Européenne d'opter pour ce principe de responsabilisation des responsables de traitement, n'est pas comparable à l'environnement social du Bénin.

### *Le principe du consentement et de légitimité du traitement*[10]

La loi indique que le consentement des personnes concernées (sauf motif dérogatoire) doit être recueilli sans préciser la forme qu'elle devrait prendre. De

[10]Articles 389 et 390 du code du numérique

plus, la preuve du consentement doit être conservée par le responsable de traitement.

Dans la mise en œuvre de ces dispositions, les responsables de traitement ont des difficultés à apporter la preuve dans les cas où le consentement est tacite.

## Les limites relatives à l'insuffisance de l'action institutionnelle

### *L'insuffisance de l'action institutionnelle*

*Une visibilité insuffisante de l'APDP*

Dans le cadre de l'exécution de sa mission, l'APDP s'active principalement à informer c'est-à-dire, conseiller les personnes sur leurs droits et devoirs en matière de traitement des données à caractère personnel. Elle garantit aussi les droits d'accès, d'opposition et de rectification, c'est-à-dire qu'elle veille à ce que les personnes accèdent facilement aux données en traitement les concernant. Aussi, assure-t-elle la veille technologique car, elle recense et vérifie le respect des données personnelles et de la vie privée à travers le contrôle des applications informatiques mises en œuvre par les responsables de traitement. Enfin, elle reçoit et instruit les affaires dont elle est saisie. Il faut également ajouter que l'Autorité donne des avis sur saisine des autorités administratives ou des organismes privés. Par ailleurs, l'APDP est depuis quelques mois très sollicitée par les organismes publics et privés. À ce titre, elle participe aux ateliers et forums de discussion relatifs au numérique, à la Cyber sécurité et à la protection des données personnelles organisés par des structures nationales et internationales. Dans une logique de sensibilisation et d'accompagnement, elle organise des séances d'information et de formation à l'intention des ministères, universités et collèges, des administrations publiques et privées et même des organisations professionnelles qui la sollicitent.

Malgré les nombreuses campagnes médiatiques et les actions que l'APDP accomplit de façon effective, elle reste méconnue de la grande majorité des béninois. Hormis les structures dans lesquelles elle a organisé ses activités, la réponse reste négative lorsque les individus sont approchés. Il se pose alors un problème de visibilité de ses actions et l'Autorité devra travailler à intensifier ses actions de communication. Cependant, il faut signaler que dans le contexte sociologique béninois, c'est beaucoup plus la répression qui oblige des individus à respecter les règles préétablies. Le renforcement des actions de contrôle et l'application ferme des sanctions pourraient donc lui valoir un début de visibilité.

## Quelques recommandations pour une gestion rassurante et sécurisante des données personnelles et de la vie privée

### *Les recommandations pour les organismes publics ou privés*

#### *Utilisation des appareils de vidéosurveillance*

La vidéosurveillance est aujourd'hui largement utilisée en entreprise pour des raisons de sécurité. Elle ne doit pas pour autant porter atteinte aux libertés individuelles et à la vie privée des salariés.

En effet, l'installation de caméras dans les locaux professionnels doit poursuivre un objectif clairement défini, légal et légitime. Le dispositif de surveillance ne doit pas entraîner un contrôle général et permanent des salariés.

Par conséquent, les caméras doivent : i) être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation ; ii) filmer les zones où de la marchandise ou des biens de valeur est entreposés. En revanche, il est interdit de filmer : i) les salariés sur leur poste de travail, sauf circonstances particulières, par exemple salarié manipulant de l'argent à condition que la caméra filme la caisse plutôt que le caissier ; ii) l'entrepôt stockant des biens de valeurs ou le coffre-fort ; iii) les zones de pause ou de repos des salariés ; iv) les toilettes ; v) les locaux syndicaux ou des représentants du personnel.

#### *Respecter les droits des salariés*

Les salariés et visiteurs doivent être informés au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance de : i) l'existence du dispositif, ii) l'identité du responsable de traitement, iii) des finalités poursuivies, iv) la base légale du dispositif (intérêt légitime de l'employeur de sécuriser les locaux), v) des destinataires des données, vi) la durée de conservation des images, vii) la possibilité d'introduire une réclamation auprès de l'APDP, viii) de la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

#### *L'accès aux données personnelles*

Seules les personnes habilitées par l'employeur, dans le cadre de leurs fonctions, peuvent visionner les images enregistrées (par exemple : le responsable de la sécurité). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéosurveillance. L'accès aux images doit être sécurisé pour éviter que tout le monde ne puisse les visionner.

#### *La durée de conservation des données personnelles*

L'employeur doit définir la durée de conservation des images issues des caméras. Cette durée doit être en lien avec l'objectif poursuivi par les caméras.

## *Les recommandations pour les personnes physiques*

### *Conseils pour les personnes adultes*

Avec le développement de l'intelligence artificielle, il est recommandé aux utilisateurs de Smartphones d'être davantage vigilants à la protection de leurs données personnelles, et de suivre certains conseils pour maîtriser les données enregistrées dans le téléphone et renforcer sa sécurité. Il s'agit de :

i) ne pas enregistrer dans le smartphone, des informations confidentielles telles que des codes secrets (ex : accès à la banque en ligne), des codes d'accès (travail, ordinateur portable) afin de limiter les risques en cas de vol, piratage, ou usurpation d'identité ;
ii) ne pas désactiver le code PIN et changer celui proposé par défaut par le constructeur en préférant un code compliqué (éviter de choisir sa date de naissance) ;
iii) mettre en place un délai de verrouillage automatique du téléphone en veille. En effet, en plus du code PIN, ce dispositif permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps, ce qui empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol ;
iv) activer si possible le chiffrement des sauvegardes du téléphone en utilisant les réglages de la plate-forme avec laquelle le téléphone se connecte. Cette manipulation garantira que personne ne sera en mesure d'utiliser les données figurant dans le smartphone ;
v) installer un antivirus quand cela est possible ;
vi) noter le numéro IMEI du téléphone pour le bloquer en cas de perte ou de vol. Ce numéro est communiqué par l'opérateur, mais il peut être relevé en tapant *#06# sur le téléphone. Il suffit alors de le conserver dans un endroit sûr ;
ne pas télécharger d'application de sources inconnues en privilégiant les plates-formes officielles ;
vii) vérifier à quelles données contenues dans le smartphone l'application installée va avoir accès ;
viii) lire les conditions d'utilisation d'un service avant de l'installer, et ne pas hésiter à consulter l'avis des autres utilisateurs ;
viii) régler les paramètres au sein du téléphone ou dans les applications de géolocalisation (Twitter, Facebook, Instagram...) afin de toujours contrôler quand et par qui l'appareil peut être géolocalisé ;
ix) désactiver le GPS ou le WIFI après utilisation de l'application de géolocalisation ;

et pour la santé (limiter l'exposition aux radiofréquences), éteindre le smartphone la nuit, ne pas le laisser de manière continue près de soi, ne pas le porter en permanence à la ceinture ou dans une poche.

## Conclusion

Le développement spectaculaire des technologies de l'information et de la communication offre de grandes possibilités et de nombreux avantages dont l'efficacité des services facilitant la vie aux populations. A l'antipode, elles constituent tout aussi de véritables dangers à la vie privée et les libertés de chacun surtout dans une société de plus en plus victimes des piratages de données personnelles avec un risque d'abus en plein essor.

Certes les mesures sont prises pour règlementer cet environnement encore nouveau pour certains afin de garantir la sécurité à tous, mais le danger subsiste et les sensibilisations doivent gagnées le terrain.

Ainsi, au-delà des aspects techniques ou juridiques inhérents aux activités numériques, la sensibilisation parait être le premier point sur lequel chaque structure se doit d'agir le plus tôt possible. Les données personnelles sont à la portée de tous faute d'une mauvaise utilisation qui devient un handicap à la protection des droits et libertés des individus. Aussi, cette sensibilisation se doit de prendre toutes les catégories socio-professionnelles en compte et surtout les couches les plus exposées aux outils du web.

Avec l'avènement du code du numérique, les entreprises et les services publics investis du pourvoir de collecter et de traiter les données personnelles des salariés, des clients ou usagers, sont tenus de faire preuve d'une plus grande vigilance dans la façon dont elles en assurent la collecte, le traitement et la protection. Les professionnels doivent par ailleurs comprendre que le droit à la vie privée dans les relations professionnelles ne saurait être considéré comme absolu. Il doit être équilibré en fonction des intérêts légitimes en jeu.

Mais au-delà du respect des règles établies, il faut espérer que les bonnes pratiques proposées en matière de protections des données personnelles, permettront d'établir entre les différents acteurs, un climat de confiance propice au développement tant souhaité et au respect des droits humain.

## Références bibliographiques