JULIEN HOUNKPE

DOCTEUR EN DROIT

FORMATION SUR LE CODE DU NUMERIQUE

+229 **95 88 79 25**

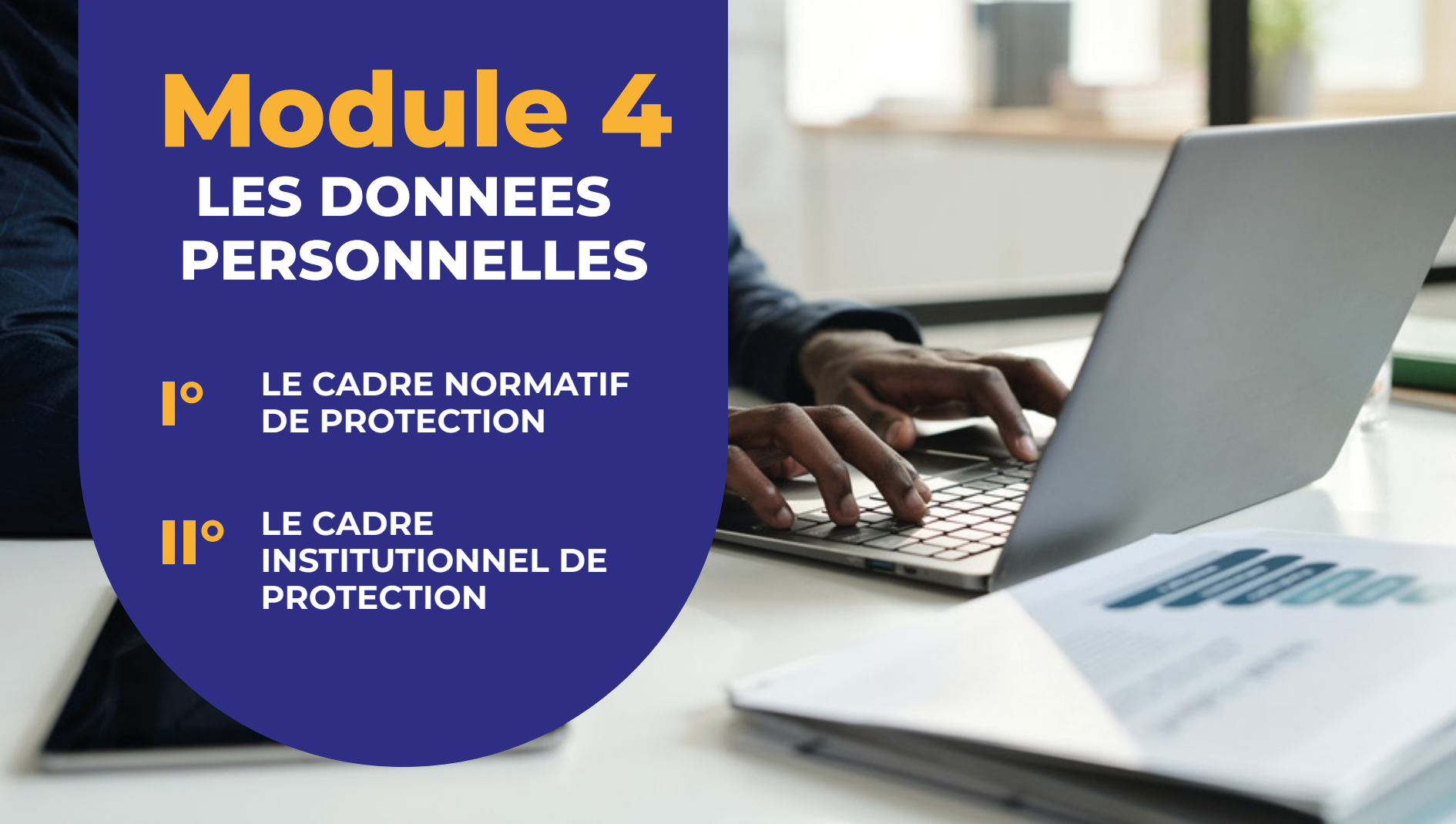
https://julienhounkpe.info

Module 4

LES DONNEES PERSONNELLES

I° LE CADRE NORMATIF DE PROTECTION

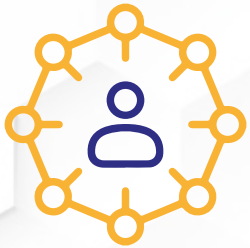
II° LE CADRE INSTITUTIONNEL DE PROTECTION



INTRODUCTION

Respect de la vie privée

Le recours aux outils technologiques nécessite l'élaboration d'un cadre juridique dont les objectifs visent à lutter contre les atteintes à la vie privée engendrées par le traitement des données personnelles. En effet, le respect de la vie privée est essentiel, notamment si elle porte sur l'intimité de l'individu.



Enjeux économiques

Les données personnelles constituent un bien précieux. Elles ont désormais une valeur marchande pour les responsables des fichiers et constituent une source d'information pour les pouvoirs publics. L'un des modèles économiques sur le numérique est leur monétisation en échange de services gratuits. Or, cette pratique entraîne des abus susceptibles de porter atteinte à la vie privée.

Donnes personnelles

Les données personnelles correspondent à toute **information de quelque nature que ce soit et indépendamment de son support, relative à une personne physique identifiée ou identifiable ou susceptible de l'être directement ou indirectement, par référence à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.**

Pratique

Cela inclut les nom, prénom, photographie, date de naissance, parenté, alliance, empreinte, adresse courriel, adresse postale, numéro de téléphone, matricule interne, immatriculation, numéro de sécurité sociale, adresse IP, identifiant de connexion informatique, empreinte numérique, enregistrement vocal, numéro de carte bancaire, groupe sanguin, code ADN, etc.

Traitement

La notion de « traitement » renvoie à toute opération, telle que « la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, ta copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel».

Exemples

Dans la pratique, un traitement correspond, par exemple, aux différents fichiers constitués pour la gestion de la clientèle d'une banque (ouverture de compte, octroi de crédit, etc), du personnel d'une Administration (salariés, gestion de carrière, etc) ou les bases de données relatives aux systèmes de contrôle d'accès à des locaux (badge, empreintes digitales, vidéosurveillance, etc.).

Paragraphe 1 : Le critère matériel

L'article 380 précise que les dispositions du livre Vième s'appliquent à :

toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé ;

tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l'exception des traitements visés à l'alinéa 2 ;

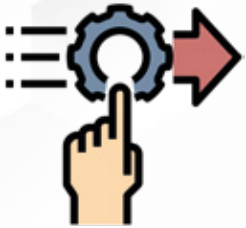
tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté et les intérêts essentiels de l'État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Paragraphe 2 : Le critère géographique

Aux termes de l'article 381, les dispositions du Livre Vième s'appliquent au traitement des données à caractère personnel effectué dans le cadre des activités d'un **responsable du traitement ou d'un sous-traitant sur le territoire de la République du Bénin**, que le traitement ait lieu ou non en République du Bénin.

Les dispositions du livre s'appliquent au traitement des données à caractère personnel relatives à des **personnes concernées qui se trouvent sur le territoire de la République du Bénin** par un responsable du traitement ou un sous-traitant qui n'est pas établi en République du Bénin.

Paragraphe 3 : les Exclusions



Activités personnelles ou domestiques

Les dispositions du Livre Vième ne s'appliquent pas aux traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques lorsque ces données ne sont pas destinées à une communication à des tiers ou à la diffusion.

Pratique

Dans la pratique, les activités personnelles et domestiques renvoient principalement aux blogs personnels et aux « pages Facebook », groupe WhatsApp, aux répertoires d'adresses personnels, aux galeries de photos, etc. Il s'agit des répertoires de nos appareils téléphoniques.

Session 2 : Les différents régimes applicables aux formalités préalables

1- le régime de déclaration [Articles 405 et 406 Code du numérique]

Régime

La déclaration préalable est une formalité à accomplir devant l'APDP par les responsables de traitement. Elle consiste à remplir et à déposer un formulaire auprès de l'APDP. Une déclaration préalable est requise pour « les traitements automatisés ou non automatisés exécutés par des organismes publics ou privés et comportant des données personnelles ». Un récépissé est délivré aux demandeurs à l'issue de l'étude du dossier.

Pratique

Dans la pratique, le régime de déclaration est appliqué aux traitements contenant des informations sur des personnes physiques réalisés à partir des systèmes d'information tels que la vidéosurveillance, les mécanismes de reconnaissances d'empreinte digitale, les badges d'identification, les systèmes d'écoute téléphonique, les cartes magnétiques, les systèmes de géolocalisation, les bases de données de personnel, de clients, de visiteurs, d'étudiants, d'élèves, etc

2. Le régime d'autorisation [Article 394 Code du numérique]

Le régime des demandes d'autorisation concerne les traitements de données susceptibles de porter atteinte à la vie privée. Lorsque le traitement concerne des données à caractère personnel sensibles, celui-ci est soumis à un régime d'autorisation.

Sont également soumis à autorisation les transferts hors de la CEDEAO [Article 391 alinéa 4] vers le reste du monde.

A l'issue de l'étude du dossier, l'APDP délivre une autorisation de traitement au postulant.

3. Le régime d’avis [Article 413 Code du numérique]

Les traitements automatisés de données personnelles opérés pour le compte de l’Etat, des établissements publics, des collectivités territoriales et des personnes morales de droit privé gérant un service public, requièrent l’avis de l’APDP avant la prise d’un acte réglementaire d’autorisation par le gouvernement.

L’ avis de l'Autorité est publié avec le décret autorisant ou refusant le traitement. L’acte d’autorisation est donné par décret pris en conseil des ministres après avis favorable de l’APDP. [Art. 411 Code du numérique]

4. Le régime de liberté

Les traitements suivants sont mis en œuvre sans formalité préalables de déclaration ou d'autorisation :

- le traitement mis en œuvre par les organismes publics ou privés pour la tenue de leur comptabilité générale
- le traitement mis en œuvre par les organismes publics ou privés relatifs à la gestion des rémunérations de leurs personnels
- le traitement mis en œuvre par les organismes publics ou privés pour la gestion de leurs fournisseurs
- le traitement mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique, ou syndical

Session 3 : Les principes gouvernant le traitement des données personnelles

1- Le principe de légitimité.

Définition.

Pour qu'un traitement soit légitime, la personne concernée doit donner son consentement de manière expresse. Il est défini comme « une manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données fassent l'objet d'un traitement manuel ou électronique ».

Pratique

Le consentement peut se manifester de différentes manières. Le plus souvent c'est par une case à cocher ou par une signature. Tout consentement doit être demandé avant la collecte des données mais doit également pouvoir être retiré à tout moment.

Les exceptions au principe de légitimité

L'exigence du consentement de la personne concernée est écartée lorsque le traitement est nécessaire :

01 au respect d'une obligation légale à laquelle le responsable du traitement est soumis, tout comme la personne concernée.

02 à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées.

03 à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande.

04 à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée

Le consentement des enfants ou majeurs protégés

Lorsque le traitement des données à caractère personnel concerne des personnes juridiquement incapables, le consentement du représentant légal est requis. En droit béninois, si la personne concernée est une personne incapable, interdite ou incapable de signer, le consentement est régi par les règles générales de droit.

2. Le principe de licéité.

Définition

Une collecte de données à caractère personnel, pour être régulière, doit être loyale, licite et non frauduleuse. Le principe est donc l'interdiction de tout traitement secret ou caché de données à caractère personnel.

Le traitement loyal suppose une totale transparence du traitement, en particulier vis-à-vis des personnes concernées et de l'autorité de protection.

La licéité suppose que le traitement soit conforme à une disposition législative ou réglementaire A titre d'exemple, la police est habilitée à collecter nos informations d'identification sans avoir à recueillir notre consentement.

Le traitement frauduleux suppose des manœuvres pour collecter des données à l'insu des personnes concernées. La fraude sur les cartes bancaires par usurpation de l'identité du titulaire du compte en est une parfaite illustration

3. Le principe de finalité

Définition

La protection des individus repose essentiellement sur le respect de la finalité du traitement déclaré auprès de l'autorité compétente. Ce principe suppose que les informations recueillies ne puissent être collectées et traitées que pour une finalité déterminée, explicite et légitime.

L'alinéa 3 de l'article 383 Code du numérique dispose que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

4. Le principe de proportionnalité

Définition

Le principe de proportionnalité exige la collecte des données strictement nécessaire à la finalité poursuivie. C'est pourquoi le législateur prévoit que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement. Le contrôle de proportionnalité repose sur l'existence d'un texte législatif ou réglementaire. A défaut, il appartient à l'APDP d'effectuer une analyse in concreto au regard des éléments du dossier.

Pratique

Dans la pratique, le principe de proportionnalité s'applique à la fois à la finalité poursuivie par le traitement et aux catégories de données collectées. Par exemple, un dispositif de vidéosurveillance ayant pour conséquence de placer le personnel sous surveillance permanente est disproportionné au regard de la finalité poursuivie.

5. Le principe d’exactitude

Définition

L'exactitude des données collectées est un gage de la qualité du traitement. Les données collectées doivent donc être exactes et, si nécessaire, mises à jour périodiquement ou lors de leur utilisation. Dans cette perspective, toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes soient effacées ou rectifiées.

Pratique

Dans la pratique, il faut dire aujourd’hui que les applications apportent elles-mêmes des solutions qui permettent d'assurer la mise à jour des informations collectées et traitées. En effet, les utilisateurs peuvent désormais modifier eux-mêmes les données qu'ils saisissent. Cette option est la plus usitée.

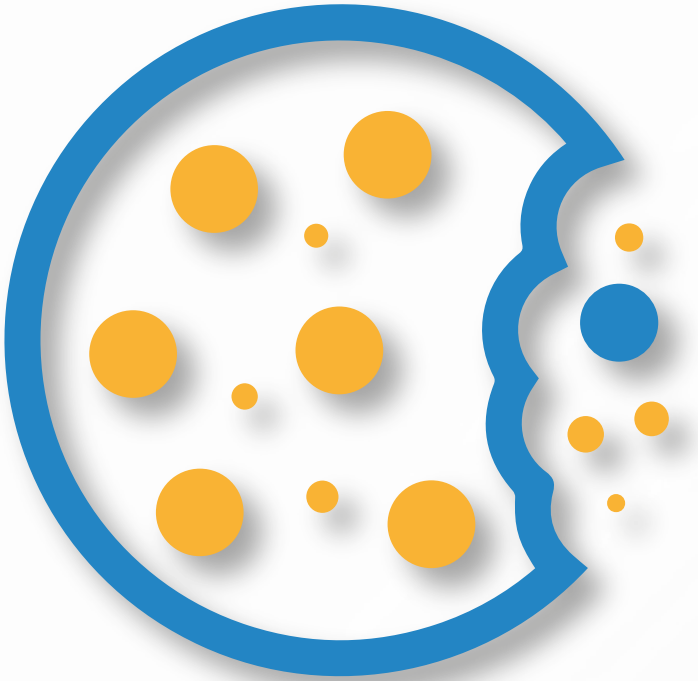
1. Le droit à l'information

Définition

Tout traitement licite des données personnelles suppose l'information des personnes concernées. Cette possibilité est offerte à la personne fichée pour qu'elle soit clairement informée sur les informations recueillies sur elle. Toute personne concernée par un traitement doit être informée, notamment de l'identité du responsable du traitement, des finalités du traitement, des catégories de données concernées, des destinataires, de la durée de conservation des données, etc.

Pratique

Cette information doit être diffusée, par exemple, au moyen d'affiches apposées dans les services recevant du public, de mentions portées sur les formulaires de collecte papier et électroniques, ainsi que sur les courriers et courriels adressés aux personnes dont les données sont collectées.



L'utilisation de cookies

Le droit à l'information devient une obligation en cas de recours à certains logiciels. Ainsi, en cas d'installation de « cookies », les personnes concernées en sont informées. Cette information doit porter sur la manière dont elles peuvent les refuser ou les supprimer.

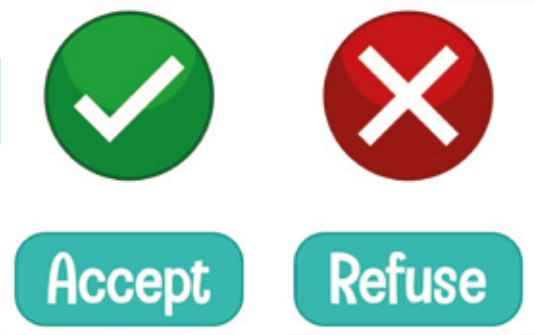
Il est de notoriété publique que les programmes cookies permettent d'affiner le profil de la personne concernée, de réaliser des statistiques d'audiences et de proposer une navigation optimale. Cette intrusion dans la vie privée des internautes oblige les administrateurs de sites internet à faire apparaître un bandeau d'avertissement.

Définition

Le droit d'accès est défini comme le droit reconnu à toute personne physique, d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir la communication, sous une forme accessible, intelligible ou compréhensible, des informations qui la concernent.

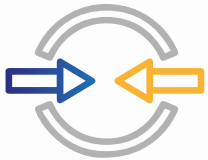
Concrètement, l'exercice du droit d'accès permet à la personne concernée de disposer d'information sur le traitement de ses données, notamment la finalité, la catégorie des données traitées, les destinataires, ou les transferts éventuels envisagés à destination d'un pays tiers.

3. Le droit d'opposition



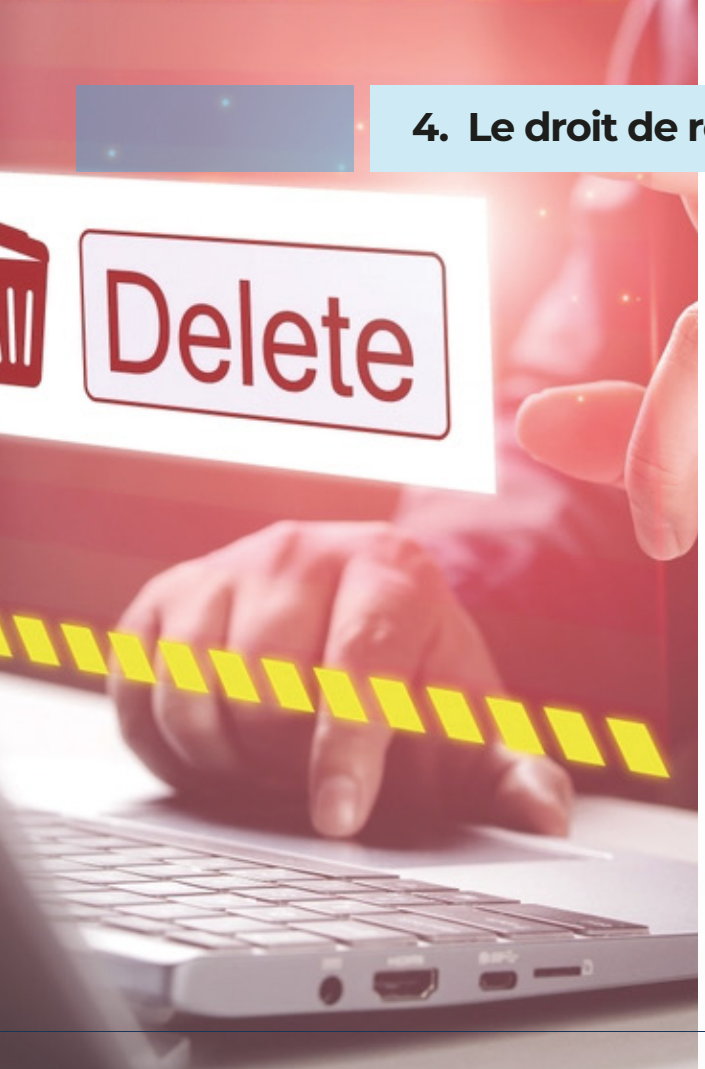
Définition

Ce principe signifie que « toute personne physique a le droit de s'opposer, pour des motifs légitimes, valables et sérieuses à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ». De plus, toute personne a le droit d'être informée avant que ses données ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection, et le droit de s'opposer, gratuitement, à ladite communication ou utilisation



Les exceptions au droit d'opposition

Le droit d'opposition n'est pas absolu. Le droit d'opposition ne s'applique pas aux traitements prévus par un acte réglementaire. A titre d'exemple, les traitements portant sur les fichiers des services fiscaux, de la sécurité sociale ou de la police en sont exceptés.



4. Le droit de rectification et de suppression

Définition

Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Pratique

A titre d'exemple, les ayants droits d'une personne décédée peuvent exiger du responsable du traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence. Cette mesure peut être appliquée aux responsables des sites Internet d'information qui ne prennent pas les précautions pour supprimer les informations relatives à une personne décédée.

1. Les obligations de confidentialité

Définition

Le traitement des données personnelles est confidentiel. Or, le recours aux outils technologiques qui nécessite l'agrégation des données personnelles entraine certaines dérives notamment en ce qui concerne leur confidentialité. La réponse à celle préoccupation est « tout responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données collectées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite».

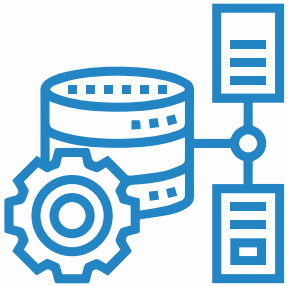
1. Les obligations de sécurité

Définition

Le recours à la technologie explique la nécessité de garantir une sécurité identique dans le monde matériel et sur les réseaux numériques. A cet effet toute personne qui effectue le traitement de données personnelles, est tenue de prendre toutes les précautions nécessaires pour assurer leur sécurité et empêcher les tiers de procéder à leur modification, à leur altération ou à leur consultation sans autorisation.

Pratique

Cette obligation se traduit donc par la nécessité de mettre en œuvre des mesures de sécurité physique (verrous aux portes, coffre-fort, etc.) et des mesures de sécurité logique (gestion des habilitations, contrôle des accès, cryptage des données, etc).



Définition

Toute donnée a une durée de vie en tant qu'information active. Elle doit être conservée pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées. Au-delà de la période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins de gestion des archives, historiques, statistiques ou de recherches.

La durée de conservation

Le Code du numérique ne définit aucune durée de conservation. Il se limite à poser un principe général aux termes duquel la durée de conservation doit être proportionnée à la finalité du traitement. Le temps de conservation des informations est défini par conséquent soit par un contrat soit par un texte légal. Cette approche laisse donc une souplesse à chaque responsable de traitement pour définir les durées adéquates. L'APDP est ainsi fondée à exercer un contrôle de proportionnalité sur toute durée déclarée ou en l'absence de précision.

2. Les obligations de pérennité

En pratique, le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données traitées peuvent être exploitées quel que soit le support technique utilisé. La négligence ne doit pas être une excuse lorsqu'il s'agit de sécurité des informations personnelles. Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à une exploitation ultérieure.

A cet effet il doit pouvoir accéder à tout moment aux données collectées et stockées malgré l'évolution des technologies. Le meilleur moyen d'y parvenir, à l'heure actuelle, est de sauvegarder périodiquement les informations sur les supports les plus récents. Le suivi de cette obligation peut être technologique.

INTRODUCTION

Autorité de protection

La sécurité des informations ne peut être une réalité que si les règles de protection sont strictement respectées. C'est pourquoi il est institué, par le Code du numérique un organisme qui, en conformité avec le système juridique interne, est chargé de contrôler le respect des dispositions législatives et règlementaires en la matière.

Plan du chapitre

L'autorité de protection des données personnelles (APDP) a un statut particulier Section 1), exerce des missions très étendues (Section 2) et disposent de larges pouvoirs coercitifs (Section 3).

1. L'indépendance de l'organisme de protection

Une autorité administrative indépendante

L'indépendance est la « clé de voûte» de l'autorité de protection. Pour remplir de manière effective sa mission, cette instance est qualifiée d'autorité administrative indépendante (AAI).

L'indépendance est garantie lorsque plusieurs critères cumulatifs sont constatés, notamment **le mode de désignation des membres, la fixation de la durée des mandats, le respect du principe de l'inamovibilité desdits mandats, l'immunité des membres, l'obligation de prêter serment ainsi que l'autonomie financière et administrative.**

L'organigramme de l'autorité de protection

Au Bénin, l'APDP est dirigée par un Bureau de trois (03) membres. L'Autorité de protection élit en son sein un Président, un Vice Président et un Secrétaire (art. 464 Code du numérique).

Sous ce format, l'organigramme de l'institution se traduit par l'existence d'un président et une session plénière des membres. Le président est secondé par des directions administratives, techniques et juridiques en charge de l'instruction des dossiers. A l'exception du président, les autres membres n'exercent pas de fonction à titre permanent.

2. L'organisation de l'autorité de protection

Composition

L'APDP est composée de huit (08) membres depuis la loi modificative de 2021 dont un bureau de deux membres (le Président et le rapporteur).

Les critères de nomination des membres

Le législateur béninois exige que les membres des autorités de protection possèdent des compétences techniques, juridiques, économiques, financières, ainsi qu'une expertise dans le domaine de la protection des droits et des technologies de l'information et de la communication.

L'origine des membres

Les membres de l'autorité de protection des données à caractère personnel viennent d'horizons divers nommés par l'Assemblée nationale, le Conseil économique et social, le Président de la République, la Cour Suprême, l'Ordre des Avocats.

1. Missions de veille

- La réception et l'examen des déclarations et des demandes d'autorisation.
- La délivrance des autorisations.
- La réception et l'instruction des plaintes, pétitions et réclamations.
- L'élaboration de règles de conduites

2. Missions d'information et de conseils

L'APDP informe et conseille les individus ainsi que les responsables de traitement de leurs droits et obligations.

- **Les missions d'information**
- **La publication d'un rapport d'activités annuel**
- **Les missions de conseils**

3. Missions de contrôle

L'autorité de protection dispose d'un pouvoir de contrôle l'autorisant à accéder aux systèmes d'information du responsable de traitement

- **Les opérations de contrôle.**
- **L'information des autorités judiciaires des opérations de contrôle.**
- **La coopération entre autorités en matière de contrôle**

1- Le pouvoir réglementaire

Pour l'accomplissement de ses missions, l'autorité de protection est habilitée à prendre des décisions d'ordre réglementaire.

2- Le pouvoir d'instruction

L'autorité de protection dispose d'un pouvoir leur permettant de procéder, sur place, sur convocation ou sur pièces, à des investigations pour vérifier la conformité d'un traitement à la législation.

2- Le pouvoir de sanction

Les traitements de données personnelles obéissent à des formalités strictes dont le non-respect est sanctionné par les autorités compétentes, notamment l'organisme de protection et le juge judiciaire. La sanction peut être d'ordre administratif ou pécuniaire.

Toute une série d'infractions liées à l'utilisation des données personnelles est prévue par l'article 460 du Code du numérique et punies d'une peine d'emprisonnement de six (06) mois à dix (10) ans et d'une amende de dix (10) à cinquante (50) millions de FCFA ou de l'une de ces deux peines seulement.

JULIEN HOUNKPE
DOCTEUR EN DROIT

+229 95 88 79 25

julien coomlan hounkpe

julienhounkpe@gmail.com

www.julienhounkpe.com