MINISTÈRE DE LA TRANSITION NUMÉRIQUE ET DE LA DIGITALISATION

ESATIC
ECOLE SUPÉRIEURE AFRICAINE DES TIC

JULIEN HOUNKPE
DOCTEUR EN DROIT

FORMATION DATA STEWARD

DROIT DES DONNEES PERSONNELLES ET DE LA CYBERSECURITE

COTONOU – LEARNING LAB, 15 - 18 AVRIL 2024

+229 95 88 79 25

https://julienhounkpe.info

PRÉSENTATION DU FORMATEUR

- Docteur en Droit, Spécialiste du Numérique
- Médiateur Professionnel et Arbitre Agréé

- Enseignant à l'Université d'Abomey Calavi (UAC)
- Chercheur au Centre de Recherche en Droit et Institution Judiciaires (CREDIJ)

- Ancien Conseiller Technique Juridique du Président de l'Assemblée nationale
- Auteur de : **Introduction au Code du numérique**, Presses Académiques Francophones, Berlin Allemagne, 2019

SYLLABUS

BENEFICIAIRES

Apprenants inscrits à la formation Data Steward de l'Ecole Supérieure Africaine des TIC.

Cette formation est ouverte aux apprenants BAC+3 dans le domaine informatique.

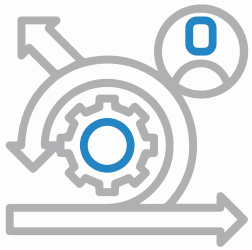
OBJECTIFS

Le module de formation permet aux participants d'acquérir des connaissances et des compétences juridiques nécessaires au métier de Data Steward.

A l'issue de ce module de formation, les participants seront capables de :

- Expliquer les concepts, principes et règles de base régissant le droit des données personnelles et de la cybersécurité ;
- Appliquer le droit des données personnelles et de la cybersécurité à des questions pratiques.

METHODOLOGIE



- Le cours sera dispensé sous la forme classique de leçons, au moyen d'une présentation magistrale.
- Chaque participant pourra compléter la formation par des travaux dirigés (TD) sous les indications du formateur.
- Modalités d'apprentissage : diapos, exposés suivis de discussion, études de cas, travaux de groupe, partages d'expérience, recherche personnelle.

PRE REQUIS

- Le module de formation appelle la lecture préalable de la Loi n° 2017-20 du 20 Avril 2018 portant Code du numérique en République du Bénin.
- Si un participant n'est pas à jour à cet égard, il devra fournir l'effort nécessaire à sa mise à niveau.

CONTENU

SEQUENCE I : Droit des données personnelles

Etape 1 – Le cadre normatif de protection des données personnelles

Etape 2 – Le cadre institutionnel de protection des données personnelles

SEQUENCE II : Droit de la cybersécurité

Etape 1 – La typologie des cyber infractions

Etape 2 – La poursuite des cyber infractions

EVALUATION

- L’évaluation sera effectuée conformément au règlement pédagogique de l’ESATIC.
- Le module de formation sera sanctionné par une moyenne pour chaque apprenant (contrôle continue et évaluation finale).

BIBLIOGRAPHIE

01 HOUNKPE (J.) Code du numérique en République du Bénin. Texte intégral introduit et présenté, Presses Académiques Francophones (PAF), Berlin Allemagne, Novembre 2019.

02 TIDJANI (F.), Guide illustré de la protection des données personnelles. Cas du Bénin. Editions Savanes du Continent, Cotonou Bénin, 2024

03 ARPAGIAN (A). La cybersécurité, PUF, Paris, 2018.

04 SCHUHL-FERAL (C.), Le Droit à l'épreuve de l'Internet, Paris Dalloz, 7ème édition, 2018.

05 GRYNBAUM (L.), LE GOFFIC (C.), MORLET HAIDARA (L.), Droit des activités numériques, Dalloz, Paris, 2014.

06 LEQUETTE (S.), Droit du numérique, Editions LGDJ Letxenso, Paris France, 2024.

SOMMAIRE

INTRODUCTION GENERALE

I- CLARIFICATION TERMINOLOGIQUE

Réglementation. Selon le Vocabulaire Juridique, la « réglementation » est l'ensemble des règles qui gouvernent une matière. En un sens plus général, c'est le droit relatif à une question. Le « droit » est une discipline sociale constituée par l'ensemble des règles de conduite qui, dans une société plus ou moins organisée, régissent les rapports sociaux et dont le respect est assuré, au besoin, par la contrainte publique.

Données. Selon le Lexique d'Information Communication, la « donnée » est la plus petite unité d'information susceptible d'etre codée sous forme numérique. Cette définition technique est exclue au profit de la « donnée personnelle » définie comme toute information qui permet, sous quelque forme que ce soit, directement ou indirectement, L'identification des personnes physiques.

I- CLARIFICATION TERMINOLOGIQUE

Cybersécurité. Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

II- SOURCES DU DROIT DES DONNEES PERSONNELLES ET CYBERSECURITE

Au Bénin, le législateur a adopté la loi n° 2017-20 du 20 avril 2018 portant Code du numérique. La loi n° 2020-35 du 06 janvier 2021 a permis au législateur béninois de réviser le Code du numérique en procédant procéder à quelques ajustements dans le texte sans en faire bouger le fond.

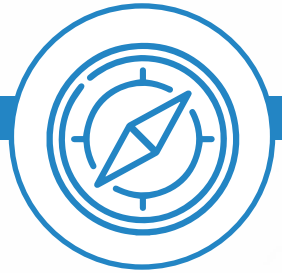
Le Code béninois du numérique consiste :

- en la modernisation des textes existants qui ont fait l'objet d'ajustements nécessaires, et
- en l'adoption de textes complémentaires sur plusieurs thématiques non encore abordées.

II- SOURCES DU DROIT DES DONNEES PERSONNELLES ET CYBERSECURITE

Composé de six cent quarante-sept (647) articles répartis en huit (08) huit livres, le Code prévoit les règles applicables :

- aux réseaux et services de communications électroniques,
- aux outils et écrits électroniques,
- aux prestataires de services de confiance,
- au commerce électronique,
- **à la protection des données personnelles,**
- **à la cybercriminalité et à la cybersécurité.**



III- GRANDES ORIENTATIONS DU MODULE

La perspective béninoise a été délibérément privilégiée pour tenir compte du Code du numérique et de la nécessité de présenter les spécificités de l'environnement national dans un contexte global.

Au regard de l'approche qui l'a inspiré, le module sur la réglementation en matière de données et cyber sécurité pourrait traverser les étapes suivantes :

- le cadre normatif et institutionnel de protection des données personnelles (Première partie),
- la typologie et la poursuite des cyber infractions (Deuxième chapitre).

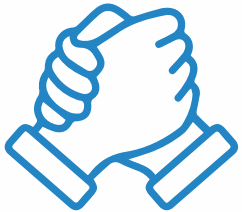
TITRE 1

LE DROIT DES DONNEES PERSONNELLES

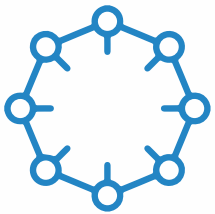
Sommaire

I-) LE CADRE NORMATIF DE PROTECTION DES DONNEES PERSONNELLES

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.

INTRODUCTION

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.

INTRODUCTION

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.).

Sequence 1 : Le champs d'application de la réglementation sur les données personnelles

Paragraphe 1 : Le critère matériel

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

01 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 ;

02 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 ;

03 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

01

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.

02

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

01

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.

02

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.

Sequence 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

Sequence 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.

1 Le principe de légitimité.

Les exceptions au principe de légitimité. L'exigence du consentement de la personne concernée est écartée lorsque le traitement est nécessaire :

- au respect d'une obligation légale à laquelle le responsable du traitement est soumis, tout comme la personne concernée.
- 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.
- à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande.
- à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée

1 Le principe de légitimité.

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.

2. Le droit d’accès

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.

01 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».*

02 Les obligations de sécurité

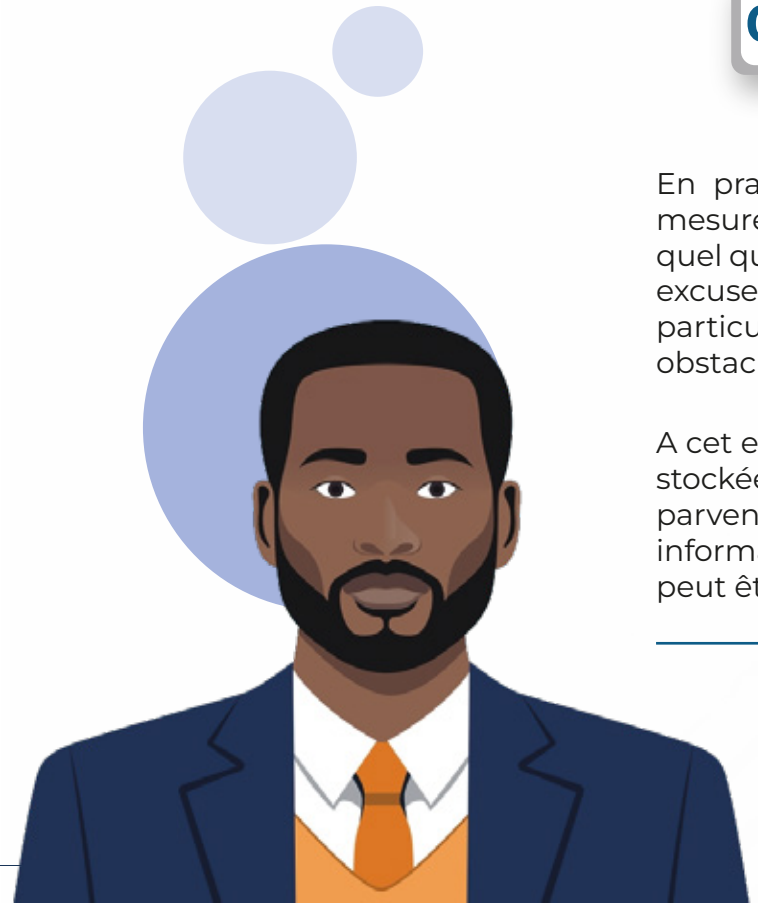
Définition. Le recours à la technologie explique la nécessité de garantir une sécurité identique dans le monde matériel et sur les réseaux numériques. A cet effet toute personne qui effectue le traitement de données personnelles, est tenue de prendre toutes les précautions nécessaires pour assurer leur 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).

03 Les obligations de conservation

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.



04 Les obligations de pérennité

En pratique, l**e 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.

II-) LE CADRE INSTITUTIONNEL DE PROTECTION DES DONNEES PERSONNELLES

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).

Section 1 : Statut de l'Autorité de Protection des Données Personnelles (APDP)

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.**

2 L'organisation de l'autorité de protection

- **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.

Section 2 : Missions de l'Autorité de Protection des Données Personnelles (APDP)

1. Missions de veille

01

La réception et l'examen des déclarations et des demandes d'autorisation.

02

La délivrance des autorisations.

03

La réception et l'instruction des plaintes, pétitions et réclamations.

04

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.

01 Les missions d'information

02 La publication d'un rapport d'activités annuel

03 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

01 Les opérations de contrôle.

02 L'information des autorités judiciaires des opérations de contrôle.

03 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.

3. Le pouvoir de sanction

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

TITRE 2

LA CYBERSECURITE

Sommaire

I-) LA TYPOLOGIE DES CYBER INFRACTIONS

INTRODUCTION

Infraction. L'infraction désigne le comportement d'une personne déterminée contraire à la loi pénale. Dans une seconde acception, plus juridique, l'infraction s'entend du comportement interdit sous la menace d'une peine définie par la loi pénale. En ce sens, l'infraction comporte deux éléments : d'une part l'incrimination, et d'autre part, la peine qui le sanctionne.

Cyber infractions. Les cyber infractions sont entendues comme désignant toute infraction qui, d'une manière ou d'une autre, implique l'utilisation des technologies informatiques. Quelle qu'en soit l'appellation, le numérique est devenue aujourd'hui le moyen de réalisation d'activités délictuelles, voire criminelles dont internet constitue désormais un vecteur privilégié de propagation.

INTRODUCTION

Plan du Chapitre. S'agissant des atteintes au système d'information, il est possible de se trouver confronté à deux hypothèses : dans la première, les cyber délinquants vont porter atteinte au système numérique de façon illicite (A), alors que dans la seconde hypothèse, l'utilisation du numérique servira de moyen pour commettre des infractions liées aux données personnelles (B).

A. Les atteintes au système numérique

- Du fait que des atteintes non autorisées peuvent causer de graves dommages et menacer la confiance dans le fonctionnement correct du système TIC, le législateur a prévu une sanction pénale pour les **atteintes aux réseaux et systèmes informatiques (C. num. béninois, art. 507 à 513).**

- La transmission non autorisée et les modifications de données, l'effacement et la destruction de données et de logiciels, de même que le fait d'entraver l'accès au système sont des infractions types de ce que l'on pourrait appeler du **« sabotage informatique » (C. num. béninois, art. 508 et 509).**

A. Les atteintes au système numérique

Les atteintes aux systèmes informatiques sont de plusieurs ordres :

01 l'accès illégal aux données et systèmes d'information (C. num. béninois, art. 507),

02 l'interception illégale des données (C. num. béninois, art. 508),

03 l'atteinte à l'intégrité des systèmes (C. num. béninois, art. 509),

04 l'atteinte à l'intégrité des données (C. num. béninois, art. 510),

05 l'abus de dispositif (C. num. béninois, art. 511),

06 la falsification informatique (C. num. béninois, art. 512),

07 la fraude informatique (C. num. béninois, art. 513).

B. Les infractions liées à l'utilisation des données personnelles

- **Envoi de message non sollicités.** Aux termes des dispositions de l'article 514 du Code du numérique, tout message électronique envoyé sur la base de la collecte de données personnelles doit contenir un lien pouvant permettre au bénéficier de se désabonner.

- **Tromperie (art. 515 Code num.).** Quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer les données personnelles est puni d'un emprisonnement de 5 ans et d'une amende de 25 millions FCFA.

- **Détournement de fonds (art. 516 Code du numérique).** Quiconque utilisera des données à caractère personnelles dans le but de détourner des fonds publics ou privé est puni d'un emprisonnement de 10 ans et d'une amende de 100 millions FCFA

B. Les infractions liées à l'utilisation des données personnelles

Toute une série d'infractions liées à l'utilisation des données personnelles est prévue par l'article 450 du Code du numérique et punies d'une peine d'emprisonement de six (06) mois à dix (10) ans et d'une amende de de dix (10) à cinquante (50) millions de FCFA ou de l'une de ces deux peines seulement.

II-) LA POURSUITE DES CYBER INFRACTIONS

INTRODUCTION

Au Bénin, la cybersécurité est définie par acte règlementaire dans le cadre de l'adoption du décret relatif à la politique de protection des infrastructures d'information critique, comme **« ensemble des mesures et des actions destinées à protéger et prévenir des dommages face aux cybermenaces. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues ».** L'une des actions phares en matière de cybersécurité est l'adoption d'une stratégie nationale de sécurité numérique (politique de cybersécurité et structures opérationnelles).

L'ampleur des réseaux informatiques, la rapidité de la réalisation des infractions et la complexité des enquêtes judiciaires (rassemblement de preuves, investigation) limitent les poursuites malgré les efforts du dispositif législatif. Conscient du danger, le législateur béninois a renforcé les moyens (A) et structures (B) d'investigation.

A. Les moyens d'investigation

- La spécificité des cyber infractions conduit à la mise en œuvre des techniques particulières d'investigation et à la participation d'experts dans le cadre des perquisitions (locaux, systèmes) et des saisies. Les interpellations et les auditions subséquentes quant à elles se font de manière classique.

- Il convient en outre d'ajouter ici des particularités en matière de prescription, d'administration de la preuve (preuve électronique, interception de données informatiques) et d'établissement des procès-verbaux électroniques.

A. Les moyens d'investigation

- **Infiltration.** Le législateur a progressivement renforcé les moyens d'investigation particulièrement adaptés à l'univers numérique avec notamment l'autorisation d'infiltration pour tout enquêteur qui découvre des agissements susceptibles de recevoir une qualification pénale sur Internet. L'autorisation d'infiltration permet par exemple d'intervenir, de façon dissimulée, sur un forum de discussion ou sur des sites.

- **Régime.** La mesure d'infiltration doit être préalablement autorisée par l'autorité judiciaire par écrit et spécialement motivée, mentionnant ainsi les infractions recherchées et l'identité de l'officier de police judiciaire responsable de l'opération. C'est le même régime qu'on applique en matière d'interception de communication

A. Les moyens d'investigation

- **Renforcement du pouvoir d'investigation au profit des autorités policières et judiciaires (art 586, 587, 588, 591 594 et 635 CdN)**

Pouvoir d'injonction de produire des documents (article 586)

Pouvoir de perquisition sans consentement (articles 587, 588)

Pouvoir d'injonction de conserver et de protéger (article 591)

Pouvoir d'interception de données informatisées (article 594)

Pouvoir d'injonction de coopérer (article 635)

B. Les structures d'investigation

1) L'Office central de lutte contre la cybercriminalité (OCRC)

OCRC OFFICE CENTRAL DE RÉPRESSION DE LA CYBERCRIMINALITÉ
POLICE RÉPUBLICAINE

Le Code du numérique a créé une structure de lutte contre les infractions cybernétiques (C. num. béninois, art. 608). Cette structure est dénommée Office central de répression de la cybercriminalité (OCRC). Elle est placée sous la tutelle du ministère en charge de la sécurité publique, a une compétence nationale.

Sont associés aux activités de cet Office, le ministère en charge de la défense nationale, le ministère en charge des finances et le ministère en charge des communications électroniques. L'Office a pour domaine de compétences les infractions spécifiques à la criminalité liées aux technologies de l'information et de la communication (C. num. béninois, art. 609)

B. Les structures d'investigation

2) L'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Dans le domaine de la cryptologie, il est créé une Agence nationale de la sécurité des systèmes d'information **« ANSSI »** (C. num. béninois, art. 604). L'Agence est en charge des missions suivantes : apporter son concours aux services de l'État en matière de sécurité des systèmes d'information et des réseaux ; effectuer un contrôle général de la sécurité des systèmes d'information et des réseaux relevant des divers organismes publics et privés identifiés par voie règlementaire ; assurer la veille technologique dans le domaine de la sécurité des systèmes d'information et des réseaux ; établir et maintenir une base de données des vulnérabilités ; diffuser des informations sur les précautions à prendre pour prévenir ou minimiser les risques d'incident ou leurs conséquences ; etc.

B. Les structures d'investigation

3) L'Agence des Systèmes d'Information et du Numérique (ASIN)

L'Agence des Systèmes d'Information et du Numérique en abrégé ASIN est un établissement public à caractère social et scientifique créé par décret No 2022-324 du 1er juin 2022 portant la fusion de l'Agence de Développement du Numérique (ADN), de l'Agence des Services et Systèmes d'Information (ASSI), de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et de l'Agence Béninoise du Service Universel des Communications Électroniques et de la Poste (ABSUCEP) et approbation de ses statuts.

L'Agence des Systèmes d'Information et du Numérique a pour mission la mise en œuvre opérationnelle des projets relatifs au secteur du numérique.

B. Les structures d'investigation

4) Le Centre national d'Investigations numériques (CNIN)

Le Conseil des Ministres en sa séance du 29 novembre 2023 a décidé de la création du Centre national d'Investigations numériques (CNIN). En effet, la nécessité impérieuse de poursuivre la lutte contre la cybercriminalité a conduit à la redéfinition des axes stratégiques implémentés jusqu'ici en vue de consolider les efforts des entités impliquées pour de meilleurs résultats.

Cette détermination s'est traduite par le recours à des technologies plus modernes, le renforcement en ressources humaines et la coordination des activités opérationnelles. En décidant de créer une structure unique constituée de multiples compétences, le gouvernement se fixe comme objectif l'efficacité plus affichée dans toutes les investigations liées à l'usage des nouvelles technologies.

Ainsi, le Centre national d'Investigations numériques (CNIN) reprendra les attributions les attributions de l'Office central de Répression de la Cybercriminalité (OCRC) et disposera de missions plus élargies absorbant partiellement celles de l'Agence des Systèmes d'Information et du Numérique (ASIN) relatives à la cybercriminalité.


JULIEN HOUNKPE
DOCTEUR EN DROIT
Merci...
+229 95 88 79 25
julien coomlan hounkpe
julienhounkpe@gmail.com
www.julienhounkpe.com

EVALUATION

QUESTIONS THEORIQUES

1) Définissez : droit, données personnelles, cybersécurité
2) Le champ d'application de la réglémentation sur les données peronnelles
3) Les différents régimes applicables aux formalités préalables
4) Les principes gouvernant le traitement des données personnelles
5) Les obligations des responsables de traitement des données personnelles
6) Les droits des personnes concernées par le traitement des données personnelles
7) Le statut de l'Autorité de protection des données personnelles (APDP)
8) Les missions de l'Autorité de protection des données personnelles (APDP)
9) Les pouvoirs de l'Autorité de protection des données personnelles (APDP)
10) Les atteintes aux réseaux et systèmes d'information
11) Les infractions liées à l'utilisation des données personnelles
12) Les moyens d'investigation dans l'environnement numérique
13) Les structures d'investigation dans l'environnement numérique

CAS PRATIQUES

Sujet 1 Champ d'application

Le Code du numérique est-il applicable au traitement des données personnelles dans chacun des cas suivants ?

a) La société ORANGE a son siège à Cotonou au Bénin, et propose ses services sur tout le territoire béninois

b) La société ORANGE a son siège à Cotonou au Bénin, mais ses services s'adressent aux personnes en dehors du Bénin

c) La société ORANGE a son siège en France et propose ses servcies aux personnes établies sur le territoire béninois

d) La société ORANGE a son siège en France et propose ses servcies aux béninois établis à New York

CAS PRATIQUES

Sujet 2 Liceité du traitement

Pour chacun des cas suivants, dites s'il s'agit d'un traitement légal de données personnelles :

a) KKR gére un media en ligne. Sur son site, il propose une newsletter pour informer ses abonnés des nouveaux articles. Pour s'abonner à la newsletter, les utilisateurs doivent remplir un formulaire en ligne et cocher une case pour donner leur consentement explicite et à recevoir des e-mails de la part de KKR.

b) Jennifer gère une boutique de vente en ligne de vêtement. Lorsqu'un client effectue un achat sur son site, elle collecte des informations personnelles telles que le nom, l'adresse et les détails de paiement pour pouvoir exécuter la commande et livrer les articles au client.

c) AK est propriétaire d'une école supérieure d'enseignement. Il est tenu, par la loi, de collecter et de traiter certaines données personnelles de ses employés pour se conformer aux obligations fiscales et sociales.

d) L'INStaD collecte des données personnelles auprès de la population dans le cadre d'un recensement officiel pour obtenir des informations démographiques et socio économiques nécéssaires à la planification et à la prise de décisions publiques.

e) Kuadio est admis à l'hopital inconscient et dans l'incapacité de forunir son consentement pour un tratement médical vital. Le personnel médical accède à ses informations de santé pour lui fournir des soins nécéssaires.

CAS PRATIQUES

Sujet 3 Détournement de finalité

Pour chacun des cas suivants, identifiez le problème juridique posé :

Cas 1 : La compagnie d'assurance ''NSIA '' propose un programme de remboursement des frais médicaux pour ses assurés. Dans le cadre de ce programme, l'assurance collecte des informations sur les antécédents médicaux des assurés afin de calculer les montants admissibles aux remboursements. La finalité légitime de la collecte de ces données est de permettre à l'assurance de fournir des remboursements précis et équitable en fonction des dépenses médicales des assurés.

Toutefois, l'assurance décide d'utiliser ces données de santé collectées à des fins différentes et non prévues à l'origine. Par exemple, elle commence à partager ces informations avec des partenaires commerciaux ou des sociétés de marketing, dans le but de cibler les assurés pour des produits ou services tiers.

Cas 2 : La société « EDF » est une entreprise qui propose des produits électroniques et informatiques. Elle a mis en place un programme de fidélité pour ses clients et obtenu leur consentement pour utiliser leurs informations personnelles, telles que leurs noms et adresses e-mail, afin de concevoir et d'envoyer des cartes de fidélité personnalisées. Les clients ont expressément donné leur accord pour participer au programme et recevoir des cartes de fidélité par e-mail.

Cependant, le service marketing de « EDF » décide de réutiliser les données personnelles pour une autre finalité sans avoir obtenu cette fois- ci leur consentement. Ils commencent à envoyer des e-mails promotionnels sur les nouveaux produits et les offres spéciales de la société sans aucun lien direct avec le programme de fidélité initial.

CAS PRATIQUES

Sujet 4 Conservation illégale de données

La société ‘’TalentTech’’ est une entreprise de recrutement qui collecte et conserve les informations personnelles des candidats pour les postes à pouvoir dans diverses entreprises clientes. Initialement, ‘’TalentTech’’ demande le consentement des candidats pour conserver leurs données pendant une période de deux ans à des fins de recontact en cas de nouvelles opportunités professionnelles.

Passé le délai de deux ans, ‘’TalentTech’’ continue de conserver les données des candidats en base active sans obtenir leur consentement pour une prolongation.

Sujet 5 Mise à jour des données

La société ’’HealthyCare’’ propose un service de santé en ligne qui permet aux utilisateurs de suivre leur santé, de prendre des rendez-vous avec des professionnels de santé, et d’accéder à des ressources médicales. Lors de l’inscription, les utilisateurs fournissent des informations personnelles telles que leur nom, leur adresse, leur date de naissance, leur groupe sanguin et leurs antécédents médicaux.

Un utilisateur de ‘’HealthyCare’’, nommé Laura, a récemment déménagé dans une nouvelle ville et a également été diagnostiquée avec une condition médicale chronique après son inscription. Ces changements affectent ses informations personnelles, y compris son adresse et son état de santé actuel.

CAS PRATIQUES

Sujet 6 Obligation de sécurité

Pour chacun des cas suivants, l'entreprise vous consulte en tant que Data Steward :

Cas 1 : (Phishing) Sarah est employée dans une entreprise de la place. Un jour, elle reçoit sur son ordinateur de travail un e-mail qui semble provenir d'un service de livraison, indiquant qu'elle doit suivre un lien pour mettre à jour ses informations de livraison. N'ayant pas reçu de formation sur la détection des e-mails de phishing, Sarah clique sur le lien malveillant, ce qui compromet la sécurité de son poste de travail et permet aux pirates d'accéder à des données personnelles sensibles de clients.

Cas 2 : (Vol de périphérique) Lors d'un déplacement professionnel, Sarah perd la clé USB dédiée à son travail contenant des données personnelles de clients. Malheureusement, les données n'étaient pas chiffrées facilitant ainsi l'accès aux informations personnelles des clients.

Cas 3 : (Accès non autorisé aux données) Sarah travaille dans le département marketing de l'entreprise et a accès à une base de données de clients. Cependant, elle utilise parfois ses privilèges d'accès pour accéder à des données personnelles d'amies et de membres de sa famille, qui ne sont pas liées à son travail. Cela constitue un accès non autorisé aux données personnelles et met en péril la sécurité de ces informations.

Cas 4 : (Vulnérabilités logicielles) Lorsque Sarah utilise son ordinateur pour accéder à la base de données de l'entreprise, elle ne met pas à jour les logiciels de sécurité et les correctifs nécessaires. Les pirates exploitent une vulnérabilité dans l'un des logiciels pour accéder aux données personnelles des clients et c'est la catastrophe !

Cas 5 : (Mauvaise gestion des mots de passe) Sarah utilise le même mot de passe pour plusieurs de ses comptes, ses comptes personnels, y compris son compte professionnel. Lorsqu'un de ses comptes personnels est compromis, les pirates utilisent le même mot de passe pour accéder à son compte professionnel, exposant ainsi les données personnelles des clients.

Cas 6 : (Manque de sauvegardes adéquates) Un jour, un virus informatique infecte le système de l'entreprise et efface une grande partie des données, y compris les données personnelles des clients. La société n'avait pas mis en place des sauvegardes régulières et sécurisées, ce qui entraine une perte permanente des données.

Sujet 7

Madame Bintou, assistante de direction à IFRI, reçoit un courriel de la Poste du Bénin concernant un colis en cours de livraison. Intriguée, Madame Bintou ouvre la pièce jointe associée. Quelques temps plus tard, le message suivant s'affiche sur son écran : « Votre ordinateur est bloqué »

1) Indiquer le (s) type(s) de cyberattaque dont elle a été victime
2) Indiquer les qualifications juridiques possibles

METHODOLOGIE JURIDIQUE

Canevas de réponse aux questions théoriques :

- Définir le(s) mot(s) clé de la question
- Règles applicables
- Analyse
- Réponse

Caneva de réponse à un cas pratique :

- Introduction : Domaine général dans lequel se situe la consultation
- Exposé des faits
- Transposition de la question en thèmes juridiques
- Formulation du ou des problèmes de droit à résoudre
- Annonce du plan

A. Règles applicables (ou principes de solutions)

i. Textes et grands principes

ii. Jurisprudences

iii. Doctrines

B. Solutions (ou réponses)

i. Exposé et explication de la solution

1. Solution du problème de droit dégagé
2. Réponses ou conseils concrets adressés au client

ii. Appréciations, discussions

1. De la solution
2. Des règles applicables