TROISIÈME FORUM NATIONAL SUR LA CYBERSÉCURITÉ ET LUTTE CONTRE LA CYBERCRIMINALITÉ

THÈME :**ADMINISTRATION PUBLIQUE ET LA PROBLÉMATIQUE DE LA PROTECTION DES DONNÉES**

PROTECTIONS DES DONNÉES ÉTATIQUE DE L'ÉTAT: QUELLE FINALITÉ?

Présenté par Monsieur **WANGUE DAVID BRICE**

Ingénieur Informaticien / Diplomate

Expert E-Government et Stratégies de Cybersécurité

Chef de la Division des Études et Projets au CENADI/MINFI

DU 10 AU 11 DÉCEMBRE 2024 ORGANISÉ PAR LE MINPOSTEL, Communauté Urbaine de Bertoua

MANDAT TDR/MINPOSTEL

- Présenter les foyers des données personnelles des agents de l'État;
- Donner les principes clés de la protection des données personnelles des agents de l'État;
- Indiquer les mesures prises par l'État et les approches adoptées pour assurer la protection des données personnelles dans le cas de l'administration électronique;
- Relever les mesures de traitements des données à caractère personnel des agents de l'État;
- Montrer les finalités de ces traitements de données;
- Présenter les stratégies mises en place pour garantir la souveraineté des données personnelles des agents de l'État;
- Faire des recommandations,

PLAN

INTRODUCTION: GÉNÉRALITÉS, PRINCIPES CLÉS ET FINALITÉS DES TRAITEMENTS DE DONNÉES

PREMIÈRE PARTIE: BREF ÉTAT DES LIEUX

DEUXIÈME PARTIE: CE QUI SE FAIT AILLEURS : ONU, UA, ALLEMAGNE, ROYAUME UNIS, SÉNÉGAL,

TROISIÈME PARTIE: MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES

QUATRIÈME PARTIE: SUGGESTIONS /RECOMMANDATIONS

INTRODUCTION

- Le développement de l'administration électronique ou « e-gouvernement » est au cœur des préoccupations de la quasi-totalité des États aujourd'hui. En effet l'administration électronique ou administration en ligne, dématérialisation ou encore digitalisation des services publics, désigne l'utilisation des technologies de l'information et de la communication (TIC) par les administrations publiques , visant à rendre les services publiques plus accessibles à leurs usagers et à améliorer les processus , la communication entre les usagers et l'administration ou entre administrations, ainsi que l'efficacité de l'administration, que ce soit sur les plans des délais, de la qualité ou de la productivité des agents publiques.

- L'état du Cameroun n'est pas en marge de cette tendance aux bénéfices multiples aux rang desquels la modernisation des services publiques avec la finalité de satisfaction de l'usager désormais vu comme « client », le renforcement de la légitimité et la souveraineté de l'État. En se dotant d'un cadre juridique sur le cyberespace dès 2010, le Cameroun affirmait ainsi sa volonté de mutation vers l'utilisation du numérique.

- Ainsi, plusieurs initiatives numériques ont vu le jour : la numérisation, la mise en ligne des documents administratifs, puis la création des sites web publics dynamique et depuis un certain temps, des services hautement stratégiques tels le passeport, le visa, le paiement de la scolarité dans les institutions publiques, la gestion des ressources humaines, la gestion des marchés publics… et très récemment la télé déclaration des impôts et taxes.

INTRODUCTION

- L'intégration et l'application des nouvelles technologies aux services publics génèrent des quantités massives de données numériques et contribue de manière significative au progrès social et à la croissance économique.
- Le rôle central des données dans le contexte de l'administration électronique nécessite d'une part une perspective politique stratégique et de haut niveau qui puisse équilibrer des objectifs politiques multiples allant de la libération du potentiel économique et social des données, mais d'autre part la prévention des préjudices associés à la collecte et au traitement de masse des données à caractère personnel.
- Il se dégage de ce qui précède, **la nécessité de protéger les données dites personnelles des acteurs de l'écosystème numérique du Cameroun, notamment, ceux de la sphère administrative publique.**
- **Quels sont les usages en matière de protection de données au Cameroun? Comment l'État en tant que garant de la souveraineté organise l'activité liée au traitement des données personnelles d'une part et, garantit la vie privée des usagers d'autre part? comment s'organise le secteur public ailleurs sur cette problématique? Quelles solutions l'administration Publique peut-elle envisager pour une protection de données efficaces et efficiente?**

GÉNÉRALITÉS SUR LA PROTECTION DES DONNÉES

- DÉFINITIONS

- **Donnée:** représentation de faits, d'informations ou de notions sous forme susceptible d'être traitée par un équipement terminal ou un programme

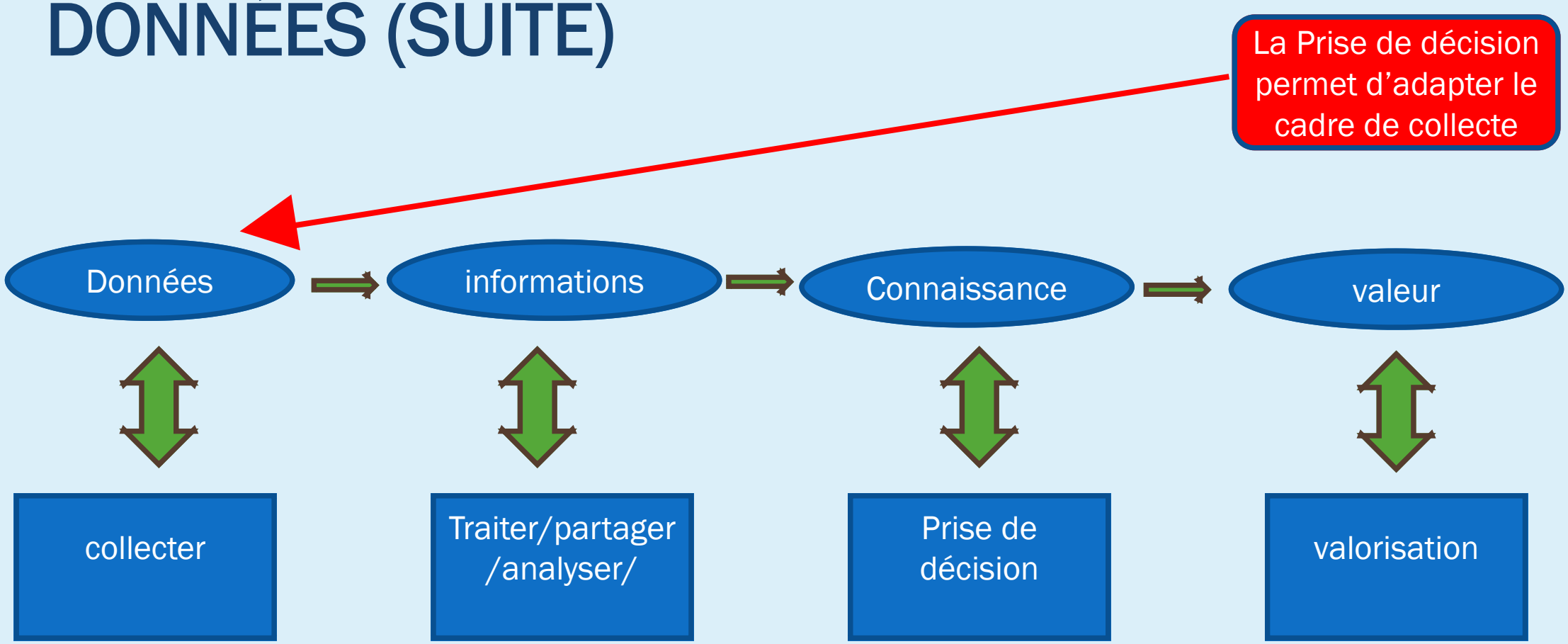
- **Donnée personnelle :** Une donnée personnelle ou « *donnée à caractère personnel* » est une **information se rapportant à une personne physique identifiée ou identifiable** (ex : nom, prénom, numéro de sécurité sociale, adresse, numéro de téléphone, adresse mail, photo, empreinte, donnée de géolocalisation, adresse IP ou identifiant en ligne).

- Une personne est dite **identifiée** lorsque l'on connaît son identité. Une personne est **identifiable** lorsqu'elle peut être identifiée, quand bien même ses nom et prénom resteraient inconnus, à partir du **croisement d'un ensemble de données** (ex : une femme vivant à telle adresse, née tel jour et membre de telle association).

GÉNÉRALITÉS SUR LA PROTECTION DES DONNÉES (SUITE)

- DÉFINITIONS
- **donnée sensible :** C'est une information relative notamment aux opinions et activités religieuses, philosophiques, politiques, syndicales, aux transactions bancaires, à l'origine raciale ou ethnique, linguistique ou régionale, à la vie sexuelle, à la génétique, à la biométrie, à la santé, aux poursuites judiciaires et aux sanctions pénales
- **information:** Tout élément susceptible d'être représenté à l'aide de conventions, pour être utilisée, traitée ou communiquée. L'information peut-être exprimée sous forme écrite, visuelle, sonore, numérique ou autre
- **connaissance:** Action, fait de comprendre, de connaître les propriétés, les caractéristiques, les traits spécifiques de quelque chose.
- **Valeur:** Ce que représente quelqu'un ou quelque chose quantitativement, financièrement ou qualitativement ou symboliquement. **Utilité et garantie**

GÉNÉRALITÉS SUR LA PROTECTION DES DONNÉES (SUITE)



Intérêt de la donnée comme base fondamentale à la prise de décision

GÉNÉRALITÉS SUR LA PROTECTION DES DONNÉES (SUITE)

DÉFINITIONS

- **Traitement de données personnelles:** Un traitement de données personnelles consiste en **toute opération portant sur des données personnelles**, quel que soit le procédé utilisé (ex : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction, le rapprochement, le verrouillage de données).
- Autrement dit, on parle de traitement de données dès que les données d'une personne sont utilisées d'une manière ou d'une autre et peu importe à qui appartiennent ces données (un **client**, un **fournisseur**, un **prestataire**, un **employé**, un **candidat à l'embauche**, etc.).
- Un traitement de données personnelles n'est pas nécessairement informatisé, **les fichiers papier sont également concernés** et doivent être protégés dans les mêmes conditions.
- **Responsable de traitement**: personne physique ou morale qui, seule ou conjointement, collecte et traite les données personnelles et en détermine les moyens et les finalités.
- Sous-traitant: Toute personne physique ou morale qui traite les données à caractère personnel pour le compte du responsable de traitement et sous ses instructions

PRINCIPES CLÉS DE LA PROTECTION DES DONNÉES

- 7 principes, constituent la pierre angulaire de la protection des données. Ils guident les organisations dans la manière dont elles **collectent, traitent et sécurisent les données personnelles.**
- **Principe 1** : Licéité, limitation des finalités, minimisation des données
- Licéité : Les données personnelles ne doivent être collectées que pour des finalités légitimes, explicites et déterminées.
- Limitation des finalités : Les données collectées ne peuvent être utilisées que pour les finalités pour lesquelles elles ont été collectées.
- Minimisation des données : La quantité de données collectées doit être réduite au minimum nécessaire pour atteindre les finalités déterminées.
- En d'autres termes, les organisations doivent être transparentes sur la raison pour laquelle elles collectent des données et ne collecter que les informations dont elles ont réellement besoin. Les mentions légales sur leur site internet sont là pour les informer.

PRINCIPES CLÉS DE LA PROTECTION DES DONNÉES (SUITE)

- **Principe 2 : Exactitude**
- Les données personnelles doivent être exactes et, si nécessaire, mises à jour. Des mesures doivent être prises pour que les données inexactes soient rectifiées ou effacées.
- Cela signifie que les entreprises doivent prendre des mesures pour s'assurer que les données personnelles qu'elles détiennent sont exactes et à jour.

- **Principe 3 : Limitation du traitement**
- Les données personnelles ne doivent être conservées que pendant une durée proportionnelle aux finalités pour lesquelles elles sont traitées.
- En d'autres termes, les entreprises doivent avoir une politique claire de conservation des données et supprimer les données lorsqu'elles ne sont plus nécessaires.

PRINCIPES CLÉS DE LA PROTECTION DES DONNÉES (SUITE)

- **Principe 4 : Intégrité et confidentialité**
- Les données personnelles doivent être traitées de manière à garantir leur sécurité, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dommages accidentels, par des mesures techniques ou organisationnelles appropriées.
- Cela signifie que les entreprises doivent mettre en place des mesures de sécurité adéquates pour protéger les données personnelles contre les accès non autorisés, les utilisations abusives et les pertes accidentelles.

- **Principe 5 : Responsabilisation** Le responsable du traitement est responsable du respect des principes susmentionnés et doit être en mesure de démontrer sa conformité.
- Cela signifie que les entreprises doivent désigner un responsable de la protection des données (DPO) qui sera responsable de la mise en œuvre et du respect de la reglementation,

PRINCIPES CLÉS DE LA PROTECTION DES DONNÉES (SUITE)

- **Principe 6 : Respect des droits des personnes**
- Les personnes ont le droit d'accéder à leurs données personnelles, de les rectifier, de les effacer, de limiter leur traitement, de s'opposer à leur traitement et de les transférer.
- En d'autres termes, les organisations doivent informer leurs clients de leurs droits en matière de protection des données et leur permettre d'exercer ces droits facilement:. **droit d'accès, droit de rectification, droit d'effacement, droit à la portabilité des données ainsi que le droit d'opposition au traitement.**

- **Principe 7 : Protection des données dès la conception et par défaut** : Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles dès la conception du traitement et tout au long des produits et services.
- Cela signifie que les organisations doivent intégrer le traitement des données dans leur stratégie globale d'entreprise.


1
FINALITÉ
Les données doivent être collectées pour un objectif précis et légitime.
2
PERTINENCE
Seules les données nécessaires à cet objectif doivent être collectées.
3
DURÉE LIMITÉE
Les données doivent être conservées uniquement le temps nécessaire à l'objectif.
4
SÉCURITÉ
Les données doivent être protégées contre tout accès non autorisé.
5
DROITS DES PERSONNES
Les personnes doivent pouvoir accéder, rectifier et s'opposer à l'utilisation de leurs données.
5 principes clés de la protection des DONNÉES PERSONNELLES

LES FINALITÉS DES TRAITEMENTS DE DONNÉES

- Un des éléments essentiels pour garantir la conformité d'un traitement de données personnelles est **la détermination préalable de la finalité**. Cette étape est essentielle dans la mesure où elle permet d'identifier les données pouvant être collectées et donc un respect effectif du principe de « minimisation des données ». Elle permet également la définition de la durée durant laquelle les données seront conservées, celles-ci ne pouvant en principe être conservées en base active que le temps nécessaire pour atteindre les objectifs concernés.
- **Pourquoi définir une finalité de traitement des données ?**
- La finalité du traitement constitue **l'objectif principal pour lequel les données personnelles sont collectées et utilisées**. Tout organisme doit dès lors, avant toute collecte de données, définir les raisons pour lesquelles il envisage de mettre en place un traitement de données personnelles.

PREMIÈRE PARTIE:

BREF ÉTAT DES LIEUX

BREF ÉTAT DES LIEUX

QUELQUES FOYERS DES DONNÉES DE L'ÉTAT

- MINREX à travers le projet E-visa
- DGSN à travers le Passeport biométrique
- MINFOPRA à travers SIGIPES, AIGLES
- MINFI à travers ANTILOPE, TELEDECLARATION des taxes, E-Bulletin
- MINMAP avec le COLEPS etc.,

BREF ÉTAT DES LIEUX

VOLET LÉGISLATIF ET NORMATIF

- La constitution
- Corpus de lois de 2010 sur le cyberespace, notamment les lois sur la communication électronique, sur la cybersécurité, sur l'accès et à l'interconnexion
- Loi du 20 juillet 2020 régissant l'activité statistique
- Loi N°2024/001 du 24 juillet 2024 sur les archives
- Loi sur la protection en ligne des enfants
- Code pénal
- Pas de loi sur spécifique sur la protection des données (processus en cours-très avancé)
- Plan de digitalisation…

BREF ÉTAT DES LIEUX

VOLET INFRASTRUCTUREL

- Existence de quelques Data center : CAMTEL, CAMPOST,
- Machine supercalculateur : Z14 au CENADI,
- Infrastructure de sauvegarde et d'hébergement des données éparses pour chaque administration : La quasi-totalité des administrations (ministère et structure autonome) ont un centre de données plus ou moins équipées en serveur robuste (salle serveur),

BREF ÉTAT DES LIEUX

VOLET ORGANISATIONNEL

- Existence des structures de régulation des TIC et administration technique dans le domaine de l'Informatique gouvernementale telles : l'ANTIC, l'ART, CENADI.
- Toutes les administrations (ministères et agences) sont acteurs à degrés différents dans le processus de traitement des données en tant que producteurs, collecteurs, analystes, utilisateurs ;
- Il n'existe pas de structure étatique dédiée à la régulation, à la gouvernance ainsi que des questions connexes à la protection des données, à l'instar d'une autorité ou une commission indépendante à la protection des données.

BREF ÉTAT DES LIEUX

VOLET RESSOURCES HUMAINES (CULTURE ET COMPÉTENCE)

Volonté du Gouvernement à faire de la digitalisation une priorité avec la création du Projet d'accélération de la transformation Numérique au Cameroun ;

Le plan de transformation digitale du Cameroun a prévu un plan qui s'articule tel que suit :

- La formation des citoyens aux usages numériques ;
- La formation des professionnels aux métiers du numérique ;
- Le renforcement des offres de formation en ligne ;
- La modernisation des centres de formation existants ;
- La consolidation d'un écosystème de formation et de recherche ;
- Le développement des formations en interne, pour les employés des entreprises et des administrations.

BREF ÉTAT DES LIEUX

VOLET RESSOURCES HUMAINES (CULTURE ET COMPÉTENCE) suite et fin

- Volonté du Gouvernement à faire de la digitalisation une priorité avec la création du Projet d'accélération de la transformation Numérique au Cameroun ;
- Faible culture des agents publics sur les enjeux et pratiques de la protection des données
- **Non appropriation des concepts majeurs tels l'anonymisation et la pseudonymisation en matière de conservation de données (stockage et hébergement) illustrée par l'utilisation parfois des données personnelles réelles en production, dans les environnements de développement ou de tests**;
- Existence d'un recueil des guides et référentiels du domaine des TIC élaboré par l'ANTIC en 2016 qui aborde du point de vue sécurité les audits de sécurité des Systèmes d'Information, la veille sécuritaire, mais pas la protection des données de manière spécifique ;
- Pas de normes ou référentiels spécifiques en termes d'interopérabilités ou d'interfaçage (API) pour le transfert des données entre les systèmes interconnectés ;

BREF ÉTAT DES LIEUX

VOLET COOPÉRATION

Le Cameroun a signé la convention de Budapest sur la lutte contre la cybercriminalité et coopère avec les instituions internationales telles que : l'UIT, l'Union Africaine, l'UNESCO

MENACES ET RISQUES CIBLANT LES DONNÉES.

Les menaces et risques sur les données se résument en la violation d'un ou de la totalité des critères fondamentaux de la sécurité /cyber sécurité à savoir la confidentialité, l'intégrité, la disponibilité et la traçabilité.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

1. Exfiltration de données

- L'*exfiltration de données* consiste à copier ou transférer sans autorisation des données hors du domaine. Ce transfert peut être effectué manuellement par une personne ayant accès aux ressources de votre organisation, ou bien il peut être automatisé et exécuté par le biais d'un programme malveillant présent sur votre réseau. Par exemple, des données peuvent être dérobées suite à la violation d'un compte (ayant donné accès aux données) ou à l'installation d'une application tierce qui envoie des données en dehors de votre domaine.

2. Fuite de données

- Une *fuite de données* est un transfert non autorisé de données sensibles en dehors du domaine. Les fuites de données peuvent se produire par l'intermédiaire des e-mails, de Meet, de Drive, de groupes ou d'appareils mobiles. Elles peuvent être dues à des comportements malveillants ou non et découler, par exemple, de l'activation de l'accès public aux groupes, de paramètres de partage sur Drive pas assez stricts, d'appareils mobiles dont la sécurité est compromise ou de pièces jointes contenues dans des e-mails sortants.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

3) Suppression de données

- La *suppression de données* est la suppression malveillante de données très difficiles ou impossibles à récupérer. Par exemple, une personne malveillante peut mettre en œuvre un rançongiciel qui chiffre vos données, puis exiger un paiement en échange de la clé de chiffrement qui permet de déchiffrer les données.

4) Attaque interne malveillante

- Une *attaque interne malveillante* est commise par un utilisateur ou un administrateur approuvé de votre organisation qui organise sciemment le transfert d'informations sensibles en dehors du domaine. Elle peut être le fait d'un employé, d'un ancien employé, d'un prestataire ou d'un partenaire. Dans ce type d'attaque, **des données peuvent être divulguées via des appareils mobiles dont la sécurité est compromise ou par l'envoi de contenu en dehors du domaine par e-mail.**

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

4) Attaque interne malveillante

- Une *attaque interne malveillante* est commise par un utilisateur ou un administrateur approuvé de votre organisation qui organise sciemment le transfert d'informations sensibles en dehors du domaine. Elle peut être le fait d'un employé, d'un ancien employé, d'un prestataire ou d'un partenaire. Dans ce type d'attaque, **des données peuvent être divulguées via des appareils mobiles dont la sécurité est compromise ou par l'envoi de contenu en dehors du domaine par e-mail.**

5) Violation de compte

- Une *violation de compte* est l'accès non autorisé au compte d'un utilisateur ou d'un administrateur du domaine. Elle se produit lorsqu'un utilisateur non autorisé dérobe des identifiants de connexion. Dans ce scénario, un compte du domaine est piraté de telle sorte qu'il peut être utilisé par une personne malveillante pour interagir avec des ressources. Le harponnage représente une méthode courante de vol d'identifiants. Dans ce cas, les pirates informatiques envoient frauduleusement un e-mail qui semble provenir d'une personne ou d'une entreprise que vous connaissez et en qui vous avez confiance.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

6) Violation de droits

- La *violation de droits* fait référence au cas où une personne malveillante réussit à pirater un ou plusieurs comptes dans votre domaine et tente de tirer parti d'autorisations limitées pour accéder à des comptes qui disposent d'autorisations plus étendues. Ce type de pirate informatique tente généralement d'accéder à des droits d'administrateur généraux pour mieux prendre le contrôle des ressources de votre domaine.

7) Cassage de mot de passe

- Le *cassage de mot de passe* est un processus de récupération de mots de passe qui s'effectue à l'aide d'un logiciel spécialisé et d'une technologie informatique de haute capacité. Les pirates informatiques sont capables de tester de nombreuses combinaisons de mots de passe dans un court laps de temps. Pour empêcher le piratage de mot de passe, une des stratégies consiste à mettre en œuvre une validation en deux étapes pour les utilisateurs et les administrateurs de votre domaine. Google verrouille également les comptes sur lesquels une activité suspecte est détectée.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

8) Hameçonnage

- L'attaque par *hameçonnage* est une pratique frauduleuse qui consiste à envoyer des e-mails semblant provenir d'entreprises réputées pour amener les personnes à révéler des informations personnelles, telles que des mots de passe et des numéros de compte, ou pour prendre le contrôle d'un compte utilisateur du domaine. Il existe trois variantes d'hameçonnage :

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces

- **Attaque par hameçonnage** : des e-mails peu ciblés sont envoyés en masse et à faible coût à de nombreux utilisateurs. Le message peut contenir un lien vers un site invitant les utilisateurs à s'inscrire pour gagner une somme d'argent ; en s'inscrivant, la victime donne ses identifiants de connexion.

- **Attaque par harponnage** : attaque ciblée contre un individu spécifique ; il peut s'agir par exemple d'inciter un comptable à ouvrir une pièce jointe qui installe un logiciel malveillant. Le logiciel permet ensuite au pirate informatique d'accéder aux données comptables et bancaires.

- **Attaque par whaling** : tentative de tromperie destinée à inciter des personnes à effectuer une action, comme un transfert d'argent. Une escroquerie par whaling consiste à faire passer un message pour un e-mail professionnel important, envoyé par des autorités légitimes.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite)

- Quelques types de menaces
- 9) Spoofing
- Le *spoofing* est la falsification d'un en-tête d'e-mail par un pirate informatique destinée à faire croire que le message provient d'une personne autre que la véritable source. Lorsqu'un utilisateur voit le nom de l'expéditeur de l'e-mail, il peut penser qu'il s'agit d'une personne qu'il connaît ou qui appartient à un domaine de confiance. Le spoofing, ou usurpation d'adresse, est une tactique utilisée dans les campagnes d'hameçonnage et de spam, car les utilisateurs de messagerie sont plus susceptibles d'ouvrir un e-mail s'ils pensent qu'il provient d'une source légitime.

MENACES ET RISQUES CIBLANT LES DONNÉES (suite et fin)

- Quelques types de menaces

10) Logiciels malveillants

- Les *logiciels malveillants* sont des logiciels conçus à des fins de piratage informatique. Il peut s'agir de virus informatiques, de chevaux de Troie, de logiciels espions ou d'autres programmes malveillants.

- **Les types de menaces techniques suscitées, combinées à certaines vulnérabilités d'ordre législative, règlementaire et organisationnel, peuvent avoir pour l'État les conséquences ci-après**

- La déstabilisation, l'espionnage, le sabotage et dans certaines conditions la cybercriminalité

LES DIFFICULTÉS LIÉES À LA SÉCURISATION DES DONNÉES DE L'ÉTAT

- *Difficultés administratives et organisationnelles*
  - Absence de responsable chargé spécifiquement de la protection des données pour chaque administration ;
  - Pas de stratégie nationale de régulation/gouvernance des données ;
  - Absence d'une structure spécifique dédiée à la protection des données ;
  - La faible culture cybersécuritaire de la majorité des agents publics

LES DIFFICULTÉS LIÉES À LA SÉCURISATION DES DONNÉES DE L'ÉTAT

- ***Difficultés administratives et organisationnelles***
  - Absence de responsable chargé spécifiquement de la protection des données pour chaque administration ;
  - Pas de stratégie nationale de régulation/gouvernance des données ;
  - Absence d'une structure spécifique dédiée à la protection des données ;
  - La faible culture cybersécuritaire de la majorité des agents publics
  - L'ethique
- ***Difficultés techniques***
  - Insuffisance des ressources humaines ;
  - Insuffisance d'infrastructures, notamment la cryptographie

DEUXIÈME PARTIE:

CE QUI SE FAIT AILLEURS

CE QUI SE FAIT AILLEURS

ONU (Organisation des Nations Unies)

L’écosystème de données à l'échelle de l'ONU vise la maximisation de la valeur de nos données, en libérant tout leur potentiel”, sa stratégie se décline telle que suit:

- Établir des bases stratégiques
- Renforcement de la prise de décision et du leadership de réflexion
- Plus grande accessibilité et un meilleur partage des données
- Une gouvernance et une collaboration améliorées pour l'impact et l'intégrité.
- Protection robuste des données de la vie privée, et le respect des droits de l'homme
- Plus grande efficacité dans les programmes, les opérations et la gestion.
- Amélioration de la transparence
- Des services améliorés axés sur les données pour les clients et les parties prenantes.

UA (Union Africaine)

Au niveau de l'Union Africaine, le Cadre stratégique en matière de données envisage le potentiel transformateur des données en vue d'autonomiser les pays africains, d'améliorer la vie des gens, de sauvegarder les intérêts collectifs, de protéger les droits (numériques) et de favoriser un développement socio-économique équitable. Les piliers majeurs sont tels que suit:

- Socle infrastructure Donner aux Africains les moyens d'exercer leurs droits par la promotion de systèmes de données fiables, sûrs et sécurisés, qui seront intégrés sur la base de normes et de pratiques communes ;
- Cadre de gouvernance Créer, coordonner et donner les moyens aux institutions de gouvernance de réguler, si nécessaire, le paysage des données en constante évolution et d'accroître l'utilisation productive et innovante des données afin de fournir des solutions et de créer de nouvelles opportunités tout en atténuant les risques ;
- Ouverture vers l'international Veiller à ce que les données puissent circuler à travers les frontières aussi librement que possible, tout en réalisant une distribution équitable des bénéfices et en traitant les risques liés aux droits de l'homme et à la sécurité nationale.

ce qui se fait ailleurs

Allemagne

La stratégie Allemande vise l'innovation par le biais de la donnée pour le progrès social et la croissance durable et ainsi renforcer la compétitivité de l'Allemagne dans l'économie numérique mondiale. Elle se décline comme ci-après:

- améliorer la fourniture de données et sécuriser l'accès aux données au niveau des infrastructures;
- promouvoir une utilisation responsable des données et exploiter le potentiel d'innovation;
- améliorer les compétences en matière de données et établir une nouvelle culture des données en Allemagne;
- faire du gouvernement fédéral un leader mondial de la nouvelle culture des données afin qu'il puisse remplir son rôle particulier dans ce domaine.

Ce qui se fait ailleurs

Royaumes unis

Les Royaumes Unis fondent leur stratégies sur deux piliers et quatre fondations :

- **Les piliers**
- Opportunités: stimuler l'innovation scientifique et technologique, et jouer un rôle clé dans la fourniture de services publics essentiels
- Identification des fondations pour sous-tendre toutes les actions stratégiques
- **Les fondations**
  - *Fondations de données: systèmes, technologies,..*
  - *Compétences en matière de données:*
  - *Disponibilité des données: open data, d'interopérabilité*
  - *Données et responsabilité: utilisation éthique, responsable, légale, sécurisée, équitable et durable*

Ce qui se fait ailleurs

Sénégal

Le Sénégal a mis sur pied une stratégie spécifique à la protection des données personnelles qui s'articulent sur les axes suivants:

- **RÉGLEMENTATION / GOUVERNANCE:** identification des axes d'amélioration du cadre réglementaire et de gouvernance de l'écosystème des données (Loi de protection de droits humains, de protection de la vie privée - autorité de régulation - …);
- **INFRASTRUCTURE:** identification des axes d'amélioration des infrastructures pour exploiter pleinement le potentiel des données (Datacenter - Cloud - supercalculateur - ouverture de données - interopérabilité…);
- **USAGES:** Identification des secteurs prioritaires que l'écosystème des données pourrait faire croître de manière significative et définir le comment (e-administration, agriculture, environnement, transport, tourisme, éducation…);
- **COMPETENCES / CULTURE:** Appréhension de la culture de la donnée dans l'administration, dans le secteur privé - adaptation des contenus de formation, …

TROISIÈME PARTIE:

MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES

LES MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES

Sur la base des guides et référentiels du domaine des technologies de l'information et de la communication élaborés par l'Agence Nationale des technologie de l'information et de la communication (ANTIC) du Cameroun, la réglementation européenne, RGPD, le cadre stratégique de l'Union Africaine en matière de données, les recommandations de la CNIL, ainsi que Recommandation du Conseil sur la protection des infrastructures d'information critiques les mesures ci-après peuvent êtres prises:

Mesures législatives , administratives et organisationnelles

- Adapter les lois existante ou en créer une spécifique;
- Doter l'État d'une institution en charge de vérifier la conformité avec le pour les organismes concernés
- L'État doit sensibiliser ses citoyens/utilisateurs sur les enjeux de la protection des données

LES MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES (suite)

- *Mesures Techniques à l'endroit des structures de traitement de données*

- Gérer les habilitations
- Sauvegarder et prévoir la continuité d'activité
- Archiver de manière sécurisée
- Encadrer la maintenance et la destruction des données
- Gérer la sous-traitance
- Encadrer les développements informatiques

LES MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES (suite)

- *Mesures techniques (suite)*

- Authentifier les utilisateurs
- Tracer les accès et gérer les incidents
- Sécuriser les postes de travail
- Sécuriser l'informatique mobile
- Protéger le réseau informatique interne

LES MESURES ET APPROCHES À PRENDRE POUR LA PROTECTION DES DONNÉES

- *Mesures techniques (suite et fin)*

- Sécuriser les serveurs
- Sécuriser les sites web
- Sécuriser les échanges avec d'autres organismes
- Protéger les locaux
- Chiffrer, garantir l'intégrité ou signer

Les structures de traitements de données doivent régulièrement procéder à une analyser d'impact de leur infrastructure de traitement, à l'effet de se rassurer de la conformité avec la réglementation en vigueur, d'où la nécessité d'un encadrement spécifique de cette question,

QUATRIÈME PARTIE:

SUGGESTIONS /RECOMMANDATIONS

SUGGESTIONS /RECOMMANDATIONS

Très Court terme:

- Finalisation de la promulgation de la loi relative à la protection des données à caractère personnel au Cameroun;
- Inscrire au plus haut niveau dans les documents de stratégies nationales, à l'instar du DSCE, de la SND30, lors des sessions de suivi-évaluation, la régulation/Gouvernance des données en tant que priorité pour le développement économique et social,
- Initier une réflexion de fond sur la construction **d'un cloud national souverain** qui pourrait servir aussi aux pays de la zone CEMAC,

Court terme:

- Réunir les responsables informatiques (DSI) des administrations au sein d'une instance permanente pour aborder les questions techniques, notamment la veille sécuritaire en matière normative: Normes sur l'interopérabilité, les API (création des interfaces entre les applications**, la pratique de minimisation, d'anonymisation et de pseudonymisation en matière de protection de données**…);

SUGGESTIONS /RECOMMANDATIONS

Court terme:

- Créer une autorité nationale indépendante de protection de données ;
- Élaborer **une stratégie nationale de régulation/gouvernance des données** ;
- Élaborer un plan de renforcement de capacités gouvernemental des responsables informatiques sur la culture cyber sécuritaire, notamment en matière de protection et sécurisation de données;
- Prévoir le poste de responsable de sécurité dans une éventuelle réorganisation des cadres organiques des administrations.

Moyen/long terme:

- **Construire un Datacenter Gouvernemental** (mutualiser, virtualiser les applications , offres de services: colocation, SaaS (Software as a Service), PaaS (Platform as a Service), DaaS (Data as a Service))

Finalité de la protection des données: garantir les droits et les libertés fondamentaux des personnes en matière de traitement de leurs informations personnelles, quelque soient leur nature , le mode d'exécution ou les responsables.

Merci pour votre aimable attention