TROISIÈME FORUM NATIONAL SUR LA CYBERSÉCURITÉ ET LA LUTTE CONTRE LA CYBERCRIMINALITÉ

THÈME :

PROTECTION DES DONNÉES PERSONNELLES: QUELLE APPROCHE POUR LES OPÉRATEURS DE TÉLÉPHONIE MOBILE ?

Bertoua, Décembre 2024

MM cxxxyuyy
ANTIC

Sommaire

Contexte :

- **L'augmentation des cyberattaques (statistiques);**

- Les données personnelles sont devenues un actif précieux dans l'économie numérique actuelle, souvent appelées "le nouveau pétrole". Les opérateurs de téléphonie mobile collectent plusieurs données sensibles;

Marché mondial des données :

- En 2022, la valeur mondiale des données personnelles était estimée à **1 400 milliards de dollars**.
- Les entreprises exploitant ces données réalisent des revenus considérables grâce à la publicité ciblée (exemple : Google et Facebook).

Contexte :

- Le respect des exigences règlementaire en matière de protection des données personnelles qui vise à garantir l'Etat que les opérateurs traitent les informations des individus de manière sécurisée, transparente et conforme aux lois applicables;

- les préoccupations des consommateurs en raison des scandales liés aux fuites de données, à la surveillance numérique, et à l'utilisation abusive de leurs informations.

Introduction (suite 1)

Comment les opérateurs de mobile peuvent-ils protéger les données personnelles de leurs utilisateurs ?

Introduction (suite 2)

- **donnée personnelle** : toutes les informations permettant d'identifier directement ou indirectement une personne.

- **les types de données personnelles :**
  - **Données d'identité (**Nom, prénom, date et lieu de naissance, nationalité, numéro tél, e-mail) ;
  - **Données financières** (numéro de compte, IBAN, historique de transaction credits, dettes) **;**
  - **Données de contact** (adresse postale perso ou prof, e-mail, numéro fixe ou mobile) **;**
  - **Données liées à l'emploi** (profession, employeur, historique de carrière, cdd/cdi, rénumération) **;**
  - **Données sensibles** (santé, biométriques, génétiques, croyance, opinions politiques)
  - **Données numériques et en ligne** (adresse Ip, login mot de passe, cookies, historique de navigation)
  - **Données de localisation** (coordonnées GPS, adresse de residence, localisation en temps reel)
  - **Données relatives aux habitudes et comportements (**Historique des achats, frequentation de lieux)
  - **Données familiales ou personnelles (**Situation matrimoniale, nom des enfants, conjoint, etc.)
  - **Données audiovisuelles (**Photographies, Vidéos, Enregistrements audio)

Introduction (suite 3)

- **quelques catégories de données personnelles collectées par les opérateurs :**
  - **d'identification et contact (**identité, coordonnées, identifiant uniques (SIM, IMEI, IMSI)) ;
  - **Facturation financières** (compte OM/MOMO, historique de transaction depots/retraits, consommation) **;**
  - **communication** (données d'appels, messages, d'usage d'internet) **;**
  - **Localisation** (cellules GSM, GPS intégré, historique de déplacement) **;**
  - **Techniques** (type d'appareil, adresse IP, Performance réseau) ;
  - **Comportementales** (habitude de consommation, préférences)
  - **Collectées pour des raisons légales** (conservation des métadonnées, enquêtes criminelles)

Introduction (suite 4)

Le rôle des opérateurs dans la collecte, le traitement et le stockage des volumes importants de données personnelles a la responsabilité :

✓**Garantir la sécurité des données** (protéger des accès non autorisés, prévenir les cyberattaques, sécuriser les cartes SIM et les communications) **;**

✓**Collecter et d'utiliser les données de manière responsable** (finalité limitée, consentement explicite, transparence) ;

✓**Conformer à la réglementation en vigueur** (loi N2010/012, N 2010/013**,** ….., 27) ;

✓**Fournir des outils et des droits aux utilisateurs** (droit d'accès, de rectification, d'effacement) **;**

✓**Sensibiliser les utilisateurs** (risques, outils de gestion, bonnes pratiques) ;

✓**Surveiller les tiers et les sous-traitants** (clause de confidentialité, partage de la responsabilité) ;

✓**Intégrer les principes de "Privacy by Design" ;**

✓**Gérer les demandes gouvernementales ;**

✓**Anticiper les évolutions technologiques.**

cadre légale et réglementaire

Cadres réglementaires majeures :

- **Convention de l'Union Africaine sur la Cybersécurité et la Protection des Données Personnelles** (adoptée en 2014) encourage les États africains à adopter des lois nationales conformes aux principes suivants :
  - Respect des droits fondamentaux, sécurité des données, consentement éclairé ;
  - Mise en place d'autorités nationales de protection des données.

- **Loi de N° 2010/012 relative à la cybersécurité et la cybercriminalité au Cameroun**
  - Article 31 (2) et Article 46 (2) l'obligation de mettre les filtres pour faire face aux atteintes préjudiciables au Données personnelles et à la vie privée des utilisateurs ;
  - Article 74 (1) et (2) est puni d'un emprisonnement de 1 à 2 ans et d'une amende de 1 à 5 000 000 pour qui porte atteinte à l'intimité de la vie privée d'autrui ou interceptent les DP lors de leur transmission ;
  - Art 32 (1),(2),(3) l'obligation des opérateurs de mobile de se soumettre au audit de sécurité obligatoire et périodique de leur SI par l'ANTIC.

- **Décret N° 2019/150 du 22 mars 2019 portant organisation et fonctionnement de l'ANTIC**

cadre légale et réglementaire (suite)

ISO/IEC 27001 : Gestion de la sécurité de l'information

- Fournit un cadre pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la sécurité de l'information (SMSI).
- Objectif : Garantir la confidentialité, l'intégrité et la disponibilité des données personnelles.

ISO/IEC 27701 : Extension pour la gestion des données personnelles spécifiquement axée sur la gestion des informations à caractère personnel (PII - Personally Identifiable Information).

- Fournit un cadre pour mettre en œuvre un **système de gestion de la protection de la vie privée (PIMS)**;
- Se conformer aux lois sur la protection des données (ex. loi N° 2010/012).

ISO/IEC 27018 : Protection des données dans le cloud

- Fournit des lignes directrices pour protéger les données personnelles traitées dans les environnements cloud.

Les risques majeurs liés aux données personnelles

- Violations de données (Data Breaches) ;
- Cyberattaques ;
- Perte ou destruction de données ;
- Exploitation des vulnérabilités ;
- Non-conformité aux réglementations ;
- Fraude et usurpation d'identité ;
- Exploitation commerciale non éthique ;
- Manipulation et désinformation ;
- Sous-traitance non sécurisée ;
- Perte de confiance des utilisateurs.

Exemples réels : CNPS, OM, Facebook

Approches et solutions pour les opérateurs

Approche technologique
Mise en place de systèmes de chiffrement des données (end-to-end encryption).
Détection des anomalies avec l'IA et l'apprentissage automatique.

Approche organisationnelle
Former les employés sur la sécurité des données.
Limiter l'accès aux informations sensibles.

Approche centrée sur l'utilisateur :
Informer clairement les clients sur l'utilisation de leurs données.
Permettre un contrôle via des portails de gestion des données.

Exemple d'initiatives concrètes

1. Mise en place d'un système de double authentification pour accéder aux données.

2. Collaboration avec des agences externes pour des audits réguliers.

3. Application permettant aux utilisateurs de vérifier et gérer les permissions.

4. Mise en place d'un tableau de bord permettant aux clients de voir quelles données sont collectées et comment elles sont utilisées.

5. Utilisation de la blockchain pour sécuriser le partage de données avec des tiers.

Conclusion & recommendations

•La protection des données personnelles est un impératif stratégique pour les opérateurs.

•Une approche combinant technologie, organisation et transparence est essentielle.

Conclusion & recommendations

•**Transparence envers les utilisateurs :** Publier des politiques de confidentialité claires et accessibles.

•**Investir dans la cybersécurité :** Augmenter les budgets alloués à la protection des données et à la formation.

•**Collaboration avec les régulateurs :** Travailler avec des Agences de régulation comme l'ANTIC au pour renforcer la conformité et la sécurité.

•**Innovation technologique :** Intégrer des technologies émergentes comme l'intelligence artificielle pour détecter les anomalies dans la gestion des données.

LA SIGNATURE ÉLECTRONIQUE

ANTIC
Agence Nationale des Technologies de l'Information et de la Communication

Merci pour votre aimable attention !

B.P: 6170 Yaoundé, Tel: +237 242 08 64 98, Fax: +237 222 20 39 31, contact: infos@antic.cm, site web: www.antic.cm