ECHANGE DE DONNEES ET COMMUNICATION

Cotonou le 07 06 22

Par Ambroise Dj. ZINSOU
Consultant formateur indépendant
Management Télécoms & TIC et Protection
des données personnelles et de la vie privée

SOMMAIRE

I. INTRODUCTION
II. CONTEXTE
III. DEFINITION
IV. CADRE LEGAL
V. ECHANGE DE DONNEES PERSONNELLES
VI. COMMUNICATION DES DONNEES PERSONNELLES

ECHANGE DE DONNEES ET COMMUNICATION

I. Définition

L'informatique, présente depuis des décennies dans les organisations publiques et privées et chez les particuliers, continue de s'y développer. Cependant, loin de l'objectif **« zéro papier »** qu'avait fait miroiter l'émergence des micro-ordinateurs, les regards se tournent dorénavant vers des objectifs d'efficience, de gain de productivité ou d'efficacité et de qualité de services qu'il pourrait apporter.. L'enjeu n'est plus dans la production massive d'informations numériques, ni dans l'automatisation à outrance des opérations pour atteindre l'objectif « zéro papier » mais plutôt dans la faculté des systèmes à organiser les informations et être à même de les échanger, communiquer rapidement sous une forme aisément compréhensible. Les échanges de données numériques prennent une place importante dans un contexte où l'efficience des organisations et la facilitation des échanges sont recherchées

ECHANGE DE DONNEES ET COMMUNICATION

2. Contexte

Avec le développement croissant des technologies de l'information et de la communication , la protection de la vie privée et des données personnelles est devenue un sujet de préoccupation majeur de nos sociétés modernes. Internet est devenu un outil incontournable de communication et d'échanges en tous genres dont les données personnelles. Par ailleurs, le développement rapide des réseaux sociaux et du e-commerce fait peser des risques sur les informations personnelles des usagers. Pour autant, lorsque les usagers « exposent » leur vie privée et données personnelles sur ces réseaux ou lorsqu'ils les « confient » à un e-commerçant pour une transaction, ils doivent être rassurés quant au traitement qui leur sera réservé.

3. Définitions

Pour une bonne appropriation du thème, certaines définitions seront nécessaires:

Communication des données personnelles

La communication des données personnelles est fondée sur le volontariat, à l'exception de la communication des données dont le traitement est exigé pour un motif légitime impérieux. (par ex.: la conclusion d'un contrat, si vous ne déclinez pas votre identité).

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

La communication est donc le fait d'établir une relation avec une autre personne ou un autre groupe en lui transmettant des messages. La transmission peut être écrite ou orale. L'émetteur (celui qui envoie le message) peut donc communiquer avec un ou plusieurs récepteurs (celui qui reçoit le message). Lorsque le récepteur est seul, on parle de communication interpersonnelle. Lorsque la communication doit atteindre plusieurs récepteurs, on parle alors de communication de groupe ou de communication de masse.

Le Code du numérique a prévu la communication des données personnes à un tiers et à la personne concernée [Art. 416 alinéa Premier et point 3 , 409.7 et 9 , 417.3].

Transmission de données personnelles : tous les transferts de données, par téléphone, télécopie, courriel ou transfert de fichiers via un réseau de communication électronique [Page 51 du CDN]

Interconnexion des données à caractère personnel : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement [p34 du CDN

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Transfert de données est toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'UEMOA [Art.391 et 392 du CDN]

État tiers : tout État non membre de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) [p28 du CDN]

Echange de données personnelles : Il s'agit d'envoi automatisé réciproque des données personnelles entre organisation via un réseau. On parle également d' échange de données informatisé [EDI], un format électronique standard qui remplace les documents physiques.

4. **CADRE LEGAL**

Il s'agit de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin [cf tous les 06 livres du Code]

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

5. ECHANGE DONNEES PERSONNELLES

5.1. Transfert de données [Art. 391 du CDN]

Le CDN présente une batterie de dispositions à suivre pour le traitement des transferts de données intra CEDEAO/UEMOA et hors. En effet, selon le CDN, est considéré comme transfert, toutes données personnelles ou fichiers de données personnelles transmis à un pays hors CEDEAO/UEMOA. Le CDN encadre précisément les transferts de données personnelles en dehors de la CEDEAO/UEMOA afin que les règles visant à les protéger continuent de s'appliquer indépendamment du pays où elles sont transférées.

Ces transferts hors CEDEAO/UEMOA sont autorisés sous réserve d'assurer un niveau de protection des données suffisant et approprié. Pour ce faire, les transferts doivent être encadrés par le biais d'outils juridiques mais aussi techniques et organisationnels.

Conformément aux dispositions de l'article 391 le transfert de données à caractère personnel vers un État tiers ou une organisation internationale ou un Etat ne peut avoir lieu que lorsque l'Autorité constate que l'État ou l'Organisation Internationale en question assure un niveau de protection équivalent à celui mis en place par les dispositions du Livre V^{ème} dont elle doit s'assurer et devra confirmer [391.1 à 3]

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Pour ce faire le responsable du traitement doitt préalablement obtenir l'autorisation de l'Autorité.

Les transferts de données à caractère personnel vers des États tiers ou une organisation internationale font l'objet d'un contrôle régulier de l'Autorité au regard de leur finalité et soumis à autorisation délivrée par l'Autorité.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Toutefois ce transfert peut se faire sous les conditions définies par l'Article 397.1 à 6 ou par décret pris en Conseil des Ministres après avis conforme de l'Autorité pour autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat et suffisant. Dans ce cas le responsable du traitement du pays récepteur devra offrir des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

5.2. Interconnexion des fichiers

L'interconnexion des fichiers visée à l'article 405 du code doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements. Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit en outre tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Trois critères permettant de déterminer si l'on est en présence d'une interconnexion ou d'un simple rapprochement de fichiers se présentent comme suit :

- En premier lieu, l'objet de l'interconnexion doit être la mise en relation de fichiers ou de traitements de données personnelles. Le fait de rapprocher des informations ou des données non personnelles ne constitue donc pas une interconnexion ;

- En second lieu, cette mise en relation doit concerner au moins deux fichiers ou traitements distincts. L'ajout d'informations dans un fichier préexistant constitue un simple rapprochement.

- Enfin, l'interconnexion doit consister en un processus automatisé ayant pour objet de mettre en relation des informations issues des fichiers ou traitements. La comparaison visuelle d'informations de fichiers différents ne constitue pas une interconnexion.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Conformément aux dispositions de l'Article 407.5, les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers sont soumis à autorisation.

5.1. Echange sécurisé

Avec le développement exponentiel des TIC, les données personnelles sont partout. Ses sources sont multiples [entreprises, personnes, puissances publiques, machines elles-mêmes] . La donnée circule, se copie, se stocke, s'agrège, se corrèle d'où l'impérieuse obligation des responsables de traitement de mettre des mesures techniques et organisationnelles en oeuvre pour la protection desdites données spécifiquement celles sensibles et qui par ailleurs représente un enjeu capital au sein de chaque structure[(entreprise privée, administration, collectivité ou cabinet libéra, etc…]. Effectivement, une attention particulière doit être portée sur la sécurisation des informations confidentielles transitant via et en dehors de l'établissement, mais également aux outils de partage utilisés, afin de garantir un échange des données sécurisé.

De ce fait, il convient de s'interroger sur les conséquences d'un transfert non sécurisé et de connaître les actions à mener pour améliorer la sécurité des échanges de données personnelles.[Art 385 du CDN]

5.4. Echange non sécurisé des données personnelles

L'échange de données ou leur transfert sans un minimum de précaution peut avoir de multiples répercussions préjudiciables à l'organisation. En effet un cybercriminel peut facilement intercepter et récupérer le contenu du message ainsi que les fichiers attachés d'où la nécessité de disposer d'un système d'échange de données sécurisé. Par exemple, la messagerie électronique ne constitue pas un moyen de communication sûr pour transmettre des données personnelles, sans mesure complémentaire. Une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des données personnelles et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, toute entité ayant accès aux serveurs de messagerie concernés [notamment ceux des émetteurs et destinataires] peut avoir accès à leur contenu.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

5.5. Le piratage des systèmes d'information

- La faille de sécurité constitue une vulnérabilité que le cyberdélinquant peut exploiter pour **accéder à l'ensemble du réseau informatique de l'organisation.** Ainsi, il prend la main sur les équipements informatiques du parc dans le but de :

- Faire cesser instantanément les activités de l'organisation ;
- Altérer l'image de marque et la crédibilité de l'organisation ;
- Fragiliser la santé financière de l'organisation[demande de rançon, perte de chiffre d'affaires, etc..] ;
- Endommager ou mettre hors services à distance les outils numériques de travail [*virus, malware, etc* …].

5.6. L'éventualité d'une perte, d'un vol ou de la revente de données

- Pleinement exploitables sans échange de données sécurisé, les données personnelles ont une **valeur marchande aux yeux du pirate.** Effectivement, ce dernier pourrait revendre les données piratées sur le dark web à un prix faramineux. Bien évidemment, les coordonnées bancaires figurent parmi les informations les plus recherchées par les pirates informatiques.

.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

Autrement, le cybercriminel pourrait purement et simplement Effacer toutes les données confidentielles par esprit de vengeance ou Publier ces informations à caractère personnel et confidentiel sur Internet.

5.7. Les mesures pour un échange de données sécurisé [Art 426 et 427 du CDN]

Dans l'optique de parer aux menaces, **une série de mesures de sécurité doit être** impérativement **déployée pour sécuriser** au maximum tout échange de documents et fichiers sensibles.

i. Sensibiliser les utilisateurs

- **informer les collaborateurs et partenaires externes sur les dangers d'un envoi de fichiers non sécurisés**

[intrusion dans le réseau informatique, usurpation d'identité, vol de données, etc]. Pour entreprendre cette démarche, plusieurs moyens de communication peuvent être exploités :

- Les newsletters ;
- Le tableau d'affichage interne ;
- Les flyers ;
- Les SMS ;
- Les réunions d'information.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

- **Rappeler les bonnes pratiques en matière de sécurité informatique** [Rédigez une charte informatique et donnez lui une force contraignante] à savoir :
  - Ne pas naviguer sur des sites non sécurisés ;
  - Ne pas cliquer sur des liens « *douteux* » ;
  - Bien vérifier l'identité de l'interlocuteur ;
  - Ne jamais communiquer ses identifiants de connexion…

ii. Gérer finement les accès aux données et fichiers confidentiels

- A**dministrer avec précision les accès aux documents partagés.**, par la mise en œuvre des solutions suivantes :
  - Possibilité d'identification du rajout d'un nouvel utilisateur ;
  - Définir les droits de consultation et de modification du fichier ;
  - Imposer un changement régulier de mot de passe ;
  - Limiter l'accès au fichier [*date d'échéance, nombre de téléchargements, etc.*] ;
  - Ajouter l'attribut « *Lecture seule* » sur le document envoyé ;
  - Mettre en place des alertes automatiques, par SMS ou par e-mail, en cas de comportement suspect d'un utilisateur ;
  - Tracer les actions réalisées sur les documents partagés.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

iii. Déployer un système d'authentification forte

- un **service d'authentification** garantira la délivrance de l'information au bon interlocuteur, tout en garantissant un échange de données sécurisé. Ce processus d'authentification se déroule en plusieurs étapes de façon à certifier l'identité numérique de l'utilisateur :
    - Identification à l'aide de la combinaison e-mail / mot de passe ;
    - Confirmation de connexion par le biais d'un code unique reçu par SMS, via une application d'authentification, par l'usage de la reconnaissance faciale, vocale ou encore des empreintes digitales ;
    - Limitation du nombre de tentatives d'accès à un compte
- En outre pour protéger l'organisation de tout accès non autorisé lors du transfert d'un fichier, l'**authentification à deux facteurs** [*2FA*] répond à la majorité des besoins des établissements privés et publics. Cependant, la technologie utilisée est susceptible de varier selon le nombre de collaborateurs, le secteur d'activité ou le type de données à sécuriser.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

iv. **Crypter les données avec un système avancé [Art 426.1]**

- Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur portable) lors d'un envoi via un réseau :
  - Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique. À ce sujet, il convient d'utiliser des fonctions cryptographiques ;
  - Utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP [Secure File Transfer Protocol], l'Applicability Statement 2 ou AS2, protocole basé sur HTTPS, SOAP (Simple Object Access Protocol) ou autres, en utilisant les versions les plus récentes des protocoles ;
  - Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).

- S'agissant de l'usage de Fax, mettre en place les mesures suivantes :

  - installer le fax dans un local physiquement contrôlé et uniquement accessible au personnel habilité ;
  - faire afficher l'identité du fax destinataire lors de l'émission des messages ;
  - doubler l'envoi par fax d'un envoi des documents originaux au destinataire ;
  - préenregistrer dans le carnet d'adresse des Fax (si la fonction existe) les destinataires potentiels.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

- Le **chiffrement des données** s'avère être une mesure essentielle notamment lorsque des données numériques sensibles sont manipulées. Cette méthode de chiffrement se résume à convertir dans un format non identifiable les données. Ce n'est qu'à la réception du message que le correspondant peut décrypter les données

Actuellement, la solution de cryptage la plus efficace reste le **chiffrement de bout en bout**. **C'**est-à-dire que les données demeurent cryptées dès l'envoi, et ce jusqu'à l'arrivée en boîte de réception chez le correspondant. À aucun moment, le message et les fichiers attachés ne sont lisibles.

v. **Privilégier une solution dédiée**

- **Mettre en œuvre une solution professionnelle d'envoi de fichiers sécurisé**. Cette dernière garantira :
  - des échanges d'e-mails et de documents entièrement sécurisés ;
  - une pleine conformité avec les disposition du livre V^{ème} (*serveurs hébergés au Bénin et ailleurs , authenticité des données, respect de la vie privée des utilisateurs, etc.*).
  - En effet, l'utilisation d'un outil gratuit de transfert soulève de nombreuses interrogations vis-à-vis de la confidentialité des informations échangées. La plupart de ces solutions tierces sont hébergées en dehors de l'espace CEDEAO/UEMOA. Elles ne sont donc pas soumises au cadre légal du Béninois et sont assez peu préoccupées par le respect de la vie privée.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

- Exploiter un algorithme reconnu et sûr, par exemple :
    - SHA-256, SHA-512 ou SHA-3 comme fonction de hachage ;
    - HMAC utilisant SHA-256, bcrypt, scrypt ou PBKDF2 pour stocker les mots de passe;
    - AES ou AES-CBC pour le chiffrement symétrique ;
    - RSA-OAEP comme défini dans PKCS#1 v2.1 pour le chiffrement asymétrique ;
    - enfin, pour les signatures, RSA-SSA-PSS comme spécifié dans PKCS#1 v2.1.
- Utiliser les tailles de clés suffisantes. Pour AES, il est recommandé d'utiliser des clés de 128 bits et, pour les algorithmes basés sur RSA, des modules et exposants secrets d'au moins 2048 bits ou 3072 bits, avec des exposants publics, pour le chiffrement, supérieurs à 65536 bits.
- Protéger les clés secrètes, au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

- Gérer les habilitations
    - Définissez des profils d'habilitation ;
    - Supprimez les permissions d'accès obsolètes ;
    - Réaliser une revue annuelle des habilitations .
- Tracer les accès et gérer les incidents:
    - Prévoyez un système de journalisation ;
    - Informez les utilisateurs de la mise en place du système de journalisation ;
    - Protégez les équipements de journalisation et les informations journalisées ;
    - Prévoyez les procédures pour les notifications de violation de données à caractère personnel.
- **Sécuriser les postes de travail :**
    - Utilisez des antivirus régulièrement mis à jour ;
    - Installez un « pare-feu » (firewall) logiciel ;
    - Recueillez l'accord de l'utilisateur avant toute intervention sur son poste.

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

- **Protéger le réseau informatique interne:**
  - Limitez les flux réseau au strict nécessaire ;
  - Sécurisez les accès distants des appareils informatiques nomades par VPN ;
  - Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi.
- **Sécuriser les serveurs**
  - Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées ;
  - Installez sans délai les mises à jour critiques ;
  - Assurez une disponibilité des données ;

ECHANGE DE DONNEES PERSONNELLES ET COMMUNICATION

5.8. VERIFICATION DU NIVEAU DE PROTECTION DES SYSTEMES DE TRAITEMENT DES DONNEES PERSONNELLES [Art. 601 à 603 du CDN]

l'Agence Nationale de la Sécurité des Systèmes d'Information est le garant de la de la sécurité des systèmes d'information et des installations des organisations. L'une de leur mission est d'alerter les organisations sur les vulnérabilités, les menaces ou la compromission de leur système.

6. COMMUNICATION DES DONNEES PERSONNELLES

La communication des données personnelles est fondée sur le volontariat, à l'exception de la communication des données dont le traitement est exigé par la loi. La loi prévoit la possibilité de communiquer les données personnelles à un tiers [416.3] ou à la personne concernée

- Si la personne décide de ne pas communiquer certaines de ses données personnelles, il peut arriver que l'organisation soit dans l'incapacité de lui accorder l'accès à un service souhaité (par ex.: la conclusion d'un contrat, si vous ne déclinez pas votre identité). {Art 417.3 du CDN]
- La communication peut être orale, sur support physique ou automatisé (Transfert de données personnelles)

JE VOUS REMERCIE