LES EXIGENCES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES RELATIONS DE SOUS-TRAITANCE ET L'OFFSHORING

APDP, 07 au 09 juin 2022

INTRODUCTION

I-) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

1. LA SOUS-TRAITANCE AU SENS DU CODE DU NUMÉRIQUE
2. LE CONCEPT DE L'OFFSHORING
3. RÉGIME DE RESPONSABILITÉ DANS LES RELATIONS RT/ST

II-) LE CHOIX DU SOUS-TRAITANT

III-) LA GESTION DE LA PROTECTION DES DONNEES DANS LES RELATIONS CONTRACTUELLES

1. GÉNÉRALITÉS SUR LES CONTRATS DE SOUS-TRAITANCE
2. SPÉCIFICITÉS DE LA SOUS-TRAITANCE DANS LES RAPPORTS DE MARCHÉS PUBLICS
   - OBLIGATION DE RESPECTER LE LIVRE 5ÈME
   - RÉFORMER LES OUTILS CONTRACTUELS DE LA COMMANDE PUBLIQUE
3. QUID DE L'OFFSHORING ?
   - LE PRIVACY SHIELD
   - LES BCR
   - SÉCURITÉ DES TRANSFERTS EN CAS D'OFFSHORING

INTRODUCTION

Les nouvelles technologies permettent de faire des données, de vraies armes décisionnelles à partir d'une science exacte des données qui conduit à une connaissance presque divine de l'être.

Elles ne sont pas néanmoins accessibles à tous ou à la portée de tous.

Les organisations sont ainsi amenées à recourir à d'autres organisations spécialisées pour profiter pleinement de leurs données.

De même, il existe des réalités moins complexes comme celle de la réduction des coûts opérationnels, les données d'une entité fille peuvent être envoyés vers une entité mère pour traitements. Là encore, il y a recours à une personne « externe » pour payer par exemple les salaires ou accorder certains avantages.

La sous-traitance est donc devenue un mécanisme usuel dans la gestion des données. Mais qu'est-ce que la sous-traitance et qu'entend-t-on par offshoring ? Comment choisir le sous-traitant dans le respect de la règlementation et comment structurer ses relations avec eux y compris en cas de transfert des données ?

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

1-) LA SOUS-TRAITANCE AU SENS DU CODE DU NUMÉRIQUE

Au sens du Code du numérique, le sous-traitant est défini comme toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement.

La sous-traitance peut donc être considérée comme l'activité par laquelle une entité juridiquement autonome met à la disposition d'une autre, son savoir-faire ou son industrie pour traiter des données à caractère personnel recueillies et détenues par cette autre entité.

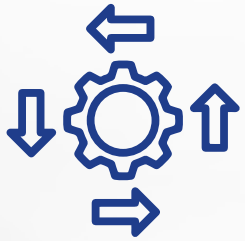
En définitive, si **sous-traitance = traiter pour le compte d'autrui**
et que **traiter = récoltées, analysées, utilisées ou stockées**

➤ **sous-traitant** = **toute personne autre que le destinataire connu ou supposé des données** mais l'ayant reçu par le biais de ce dernier afin d'atteindre des objectifs que ce même lui a fixé.

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

1-) LA SOUS-TRAITANCE AU SENS DU CODE DU NUMÉRIQUE

Autrement dit, le sous-traitant c'est le :



intégrateur web externe

concepteur externe de base de données

prestataire de services de numérisation de documents

prestataire de services d'archivage

Hébergeur web

agence marketing

fournisseur de solutions de stockage cloud

propriétaire du système d'informations interne

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

2-) LE CONCEPT DE L'OFFSHORING

Le Code du numérique ne définit pas le concept de l'offshoring.

L'offshoring désigne le fait de confier la gestion et la réalisation d'un service auparavant effectué dans le pays d'origine de l'entreprise, à une autre entreprise, cette fois-ci étrangère, et cela qu'il s'agisse ou non d'externalisation.

Il s'agit généralement d'un processus opérationnel, comme la fabrication, ou des processus connexes, comme la comptabilité. Plus récemment, l'offshoring a été associé principalement à l'externalisation de services techniques et administratifs et marketing comme c'est le cas pour le service après-vente.

Les progrès techniques dans le domaine des télécommunications ayant amélioré les possibilités de commerce des services, l'Inde est devenue l'une des principales destinations en termes d'offshoring, même si de nombreuses régions du monde sont en train d'elles aussi devenir des destinations offshores, comme l'Asie du sud-est ou plus récemment, certains pays d'Afrique dont le Maroc et encore plus récemment le Bénin avec notamment les centres d'appels et la Zone Industrielle de Glo-Djigbé.

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

2-) LE CONCEPT DE L'OFFSHORING

Ce procédé a cela de particulier qu'il va ramener dans un environnement juridique donné les activités d'une entité opérant techniquement dans un environnement juridique différent. C'est d'ailleurs par ce biais que le Code du numérique s'y invite.

En effet, en délimitant le champ d'application territorial du livre 5ème, l'article 381 du Code dispose que « les dispositions du présent Livre 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…** ».

Il va sans dire que toute activité de traitement se déroulant sur le territoire béninois est soumis aux dispositions du livre 5ème. En tout état de cause, les activités d'organisations offshores établies au Bénin sont concernées par le Code du numérique.

Poursuivant toutefois, l'article 381 étend également son champ d'application 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…** ».

De ce point de vue, **la société offshore opérant depuis l'étranger sur des données de personnes concernées se trouvant au Bénin** est concernée par le livre 5ème du Code avec cela de particulier qu'elle se trouve dans l'obligation d'être à la fois conforme aux dispositions nationales et aux dispositions de son pays d'origine si celui-ci dispose d'une règlementation spécifique.

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

3-) RÉGIME DE RESPONSABILITÉ DANS LES RELATIONS RT/ST

D'abord, relevons que lorsqu'une société offshore accepte de traiter des données à caractère personnel pour « le compte d'un responsable de traitement », elle se retrouve dans la même situation juridique que le sous-traitant, prestataire « local ». La société offshore n'est donc pas juridiquement installée dans un no man's land du fait de sa délocalisation. Elle doit encore se conformer aux lois de son pays d'origine mais également aux lois du pays hôte et aux lois qui s'appliquent à elles du fait de ses activités.

Ensuite, relevons que les attaques informatiques prennent parfois des voies détournées pour atteindre leur cible finale. Les sous-traitants sont de bons canaux pour les cyberattaquants. Paradoxalement, la plupart des organismes ont donc le sentiment d'être à l'abri une fois qu'ils ont sous-traité. Ils ne se préoccupent ainsi pas toujours d'aller vérifier ce qu'il en est chez leurs sous-traitants et s'aperçoivent souvent tardivement que leurs prestataires délèguent eux-mêmes une partie des opérations de maintenance à un second prestataire situé par exemple en Inde, et dont l'approche en matière de sécurité est totalement différente.

Or, lorsqu'un responsable de traitement recourt à un sous-traitant, il n'est ni déchargé de sa responsabilité sur les données qu'il traite, ni allégé de ses obligations au titre de ses activités de traitement.

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

3-) RÉGIME DE RESPONSABILITÉ DANS LES RELATIONS RT/ST

La défaillance du sous-traitant qui lui est imputable pourrait alors bien être plus lourde qu'une simple perte des données ou du paiement d'une rançon. Il encourt aussi des sanctions financières lourdes (jusqu'à F CFA 100 000 000), un risque réputationnel et donc d'atteinte à son image aux fortes conséquences (perte de confiance des clients, baisse du chiffre d'affaires, etc.). Pis, aux termes de l'article 461 du Code, « Le responsable de traitement ou son représentant sera passible du paiement des amendes encourues par son sous-traitant ».

Dans ce contexte, il est important de bien encadrer juridiquement les relations entre responsables de traitement et sous-traitants.

Cependant, les responsables de traitement et le sous-traitant, cocontractants pour le traitement des données, disposent d'une **action récursoire** l'un contre l'autre « ...lorsqu'un responsable du traitement ou un sous-traitant a, conformément à l'alinéa 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur

I°) RECONNAITRE LE SOUS-TRAITANT ET L'OFFSHORING

3-) RÉGIME DE RESPONSABILITÉ DANS LES RELATIONS RT/ST

part de responsabilité dans le dommage, conformément aux conditions fixées à l'alinéa 2. » (article 451).

Mais si les sous-traitants se retrouvent à bien d'endroits en situation de responsabilité partagée avec le responsable de traitement comme au chapitre de l'obligation de sécurité des données à caractère personnel (article 426) partagée par les deux acteurs du traitement, **la responsabilisation des sous-traitants n'amoindrit pas les obligations du responsable de traitement**, qui demeure le seul responsable quant au choix de son sous-traitant.

L'article 386 du Code dispose en effet, que le responsable de traitement doit « ...1. choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements, notamment pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées ; et 2. veiller au respect des mesures du point i. ci-dessus, notamment par la stipulation de mentions spécifiques dans les contrats passés avec des sous-traitants...».

En application du principe d'Accountability, le responsable de traitement doit être en mesure d'apporter la preuve, que le choix du sous-traitant a été fait sur la base de « garanties suffisantes

II°

LE CHOIX DU SOUS-TRAITANT

LES EXIGENCES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES RELATIONS DE SOUS-TRAITANCE ET L'OFFSHORING

II°) LE CHOIX DU SOUS-TRAITANT

L'article 386 du Code guide sur les critères qui doivent entrer en ligne de compte au moment de choisir son sous-traitant.

Il dispose en effet que « ...lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en République du Bénin, doit : 1. choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements, notamment pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées... ». Toutefois, qu'entend-on par « garanties suffisantes » ?

L'article 426 du Code apporte une réponse générique : « ...il incombe également au responsable du traitement, son représentant ainsi qu'au sous-traitant de veiller au respect de ces mesures de sécurité. Ces mesures peuvent notamment comprendre :

1. la pseudonymisation et le chiffrement des données à caractère personnel ;
2. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
3. des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
4. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.»

II°) LE CHOIX DU SOUS-TRAITANT

Ces considérations, très générales, n'ont pas fait l'objet de précisions détaillées mais on peut toutefois retrouver quelques éléments au sein de la pratique dédiée.

Il est apparu nécessaire de procéder à une approche globale de l'évaluation d'un sous-traitant, tenant d'abord compte des exigences du Livre 5ème vis-à-vis de lui. En se basant sur le Code, on peut identifier les exigences pesant sur celui-ci. Parmi elles, on dénombre :

- La présence d'un DPO ;
- La formation/sensibilisation de ses salariés aux enjeux de la protection des données personnelles ;
- L'existence de registre de procédure de gestion des registres et des traitements ;
- La gestion et le contrôle de la conformité des sous-traitants ultérieurs ;

- La localisation du traitement des données personnelles ;
- Le transfert de données personnelles hors CEDEAO ;
- Les mesures techniques de protection des données personnelles ;
- Les mesures organisationnelles de protection des données personnelles ;

- La gestion des droits des personnes ;
- La prise en compte des principes de protection des données « Privacy by design » et « Privacy by default » ;
- L'adhésion à un code de conduite ;
- L'obtention d'une certification.

II°) LE CHOIX DU SOUS-TRAITANT

Certains de ces critères ont une importance particulière. C'est le cas des mesures techniques et de la localisation des données. D'autres critères n'emportent pas le même consensus : la présence d'un DPO est fondamentale pour certains, alors que d'autres y attachent une importance secondaire.

En tout état de cause, il est difficile d'établir une liste exhaustive des critères de contrôle d'un sous-traitant et de les classer par ordre de priorité.

En pratique, l'expertise d'un sous-traitant peut s'apprécier de différentes manières, telles que :

- l'application par le sous-traitant d'un code de bonne conduite,
- la vérification de la conformité de son site internet,
- la démonstration que le produit et/ou service prend en compte le privacy by design et le privacy by default ou encore
- via une la documentation sur les mesures de sécurité.

II°) LE CHOIX DU SOUS-TRAITANT

Pour ce qui est de la fiabilité, il peut être recommandé de prendre en compte :

- la renommée sur le marché du sous-traitant,
- la date de création de l'entreprise,
- sa présence à l'international ou
- ses certifications (ISO27001, ISO27701, etc.).

Concernant les ressources, la présence d'un DPO chez le sous-traitant ou la formation/sensibilisation du personnel à la protection des données sont des facteurs à prendre en compte et facilement vérifiables.

D'un point de vue opérationnel, le responsable de traitement devrait établir un questionnaire contenant toutes les informations qu'il juge utiles pour s'assurer que le sous-traitant présente des garanties suffisantes et intégrer l'usage de ce questionnaire dans un process interne relatif au choix d'un nouveau prestataire.

LE CHOIX DU SOUS-TRAITANT

- *Avez-vous désigné un Délégué à la Protection des Données ?*
- *Avez-vous établi un registre des activités de traitement Responsable de traitement et Sous-traitant ?*
- *Avez-vous une Politique de Sécurité ?*

- *Avez-vous mis en place une procédure de gestion de crise, notamment en cas de violation de données ?*
- *Votre personnel est-il formé/sensibilisé à la protection des données ?*
- *Proposez-vous un Plan d'Assurance Sécurité ?*

II°) LE CHOIX DU SOUS-TRAITANT

En analysant les réponses obtenues, le responsable de traitement est désormais en mesure de faire une présélection des sous-traitants, pour ne retenir que ceux démontrant un bon niveau de maturité en matière de protection des données.

Mais un second tri devra être réalisé par le responsable de traitement, à partir d'autres points de contrôle. Ainsi le choix du sous-traitant devrait être conditionné à la réalisation des étapes suivantes :

- **La réalisation d'une étude de risque sur la sécurité des données pouvant avoir des impacts sur la vie privée**

  Ce procédé lui permet d'une part d'identifier les mesures techniques et organisationnelles de sécurité à mettre en place et d'autre part de documenter la conformité de son traitement.
  Si l'étude révèle des risques, cela signifie qu'il est nécessaire de mettre en place des mesures de sécurité pour réduire ce risque.

- **L'identification des mesures techniques et organisationnelles de sécurité les plus adaptées aux risques identifiés**

  Une fois ce travail réalisé, le responsable de traitement dispose d'une liste exhaustive des mesures techniques et organisationnelles de sécurité.

II°) LE CHOIX DU SOUS-TRAITANT

- **La vérification que le sous-traitant est en mesure de mettre en place les mesures techniques et organisationnelles de sécurité.**

  Afin de s'assurer que le ou les sous-traitants sélectionnés appliquent déjà ou sont en mesure d'implémenter les mesures de sécurité identifiées, le responsable de traitement peut leur adresser un document sous forme de questionnaire reprenant l'ensembles desdites mesures. Par ailleurs, le responsable de traitement peut s'appuyer sur l'ensemble de ces exigences pour conditionner le recours à un sous-traitant de second rang.

  ➤ **Vérifier la chaîne de sous-traitance**

  Il est souvent constaté dans les modèles de contrats fournis par les sous-traitants qu'ils se réservent la possibilité de faire eux-mêmes appel à un sous-traitant de second rang afin de déléguer une partie des opérations de traitement. Si bien souvent le contrat contient l'obligation pour le sous-traitant d'en informer au préalable le responsable de traitement pour lui permettre d'émettre des objections, dans les faits ce dernier en a rarement connaissance.

  Il est donc fortement recommandé que le responsable de traitement prenne en compte la chaine de sous-traitance au moment de sélectionner un sous-traitant et de bien l'encadrer contractuellement.

II°) LE CHOIX DU SOUS-TRAITANT

- **Audit régulier des prestataires**

  Si l'audit n'est pas obligatoire, ce dernier reste un instrument efficace permettant l'assurance du maintien de la visibilité des pratiques du sous-traitant.

  Il est fortement conseillé de mettre en pratique régulièrement une clause contractuelle d'audit (au moins une fois par an).

Si aucun des points ci-dessus ne permet à lui seul d'apprécier « les garanties suffisantes », cela constitue néanmoins un faisceau d'indices qui peut être utilisé pour faire une présélection des sous-traitants.

Une fois le sous-traitant choisi, il faut bien gérer la relation contractuelle.

III°

LA GESTION DE LA PROTECTION DES DONNEES DANS LES RELATIONS CONTRACTUELLES

LES EXIGENCES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LES RELATIONS DE SOUS-TRAITANCE ET L'OFFSHORING

III°) LA GESTION DE LA PROTECTION DES DONNEES DANS LES RELATIONS CONTRACTUELLES

La gestion de la protection des données dans les relations contractuelles peut se faire dans un cadre général ou spécifique tout en prenant en compte les cas de transfert de données à l'étranger en présence des cas d'offshoring.

1-) GÉNÉRALITÉS SUR LES CONTRATS DE SOUS-TRAITANCE

C'est l'article 386 du Code qui pose le principe de l'obligation de contractualiser la relation avec le sous-traitant.

Il impose au responsable de traitement, de « fixer dans le contrat » les responsabilités du sous-traitant vis-à-vis de lui notamment pour la protection de la sécurité et de la confidentialité des données.

L'article 426 renchérit en demandant expressément que « le choix du sous-traitant et les modalités du contrat liant celui-ci avec le responsable du traitement » soient « soumis aux dispositions du présent Livre ».

Au regard de ces considérations, en pratique, le contrat de sous-traitance doit alors refléter les modalités de « report » des responsabilités du responsable de traitement sur le sous-traitant.

Autrement dit et pour en alléger le sens, le contrat de sous-traitance va encadrer les modalités de « coopération et d'assistance » du responsable de traitement dans sa conformité aux dispositions du livre. Par ce contrat, le sous-traitant est tenu en quelque sorte pour « coresponsable » ou « garant par mandat » de la conformité du responsable de traitement.

1-) GÉNÉRALITÉS SUR LES CONTRATS DE SOUS-TRAITANCE

Le sous-traitant doit ainsi démontrer une certaine capacité technique et organisationnelle pour permettre au responsable de traitement de satisfaire convenablement à ses obligations en matière de protection.

Un cadre contractuel approprié sera donc nécessaire pour préciser l'objet et la durée du traitement confié au sous-traitant, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, en tenant compte des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée.

L'article 386 offre un aperçu des points qui doivent être convenus entre un responsable du traitement et un sous-traitant. Ce contenu condensé trouve des repères à la lecture des obligations dont le responsable de traitement est lui-même tenu et permet de découvrir l'ensemble des thèmes qui pourront apparaître dans les contrats entre responsables de traitements et sous-traitants, en même temps que les engagements qui doivent apparaître dans les contrats entre responsables de traitement et personnes concernées.

De manière générique, le contrat de sous-traitance doit mentionner

- la ou les finalités du traitement (article 435 Al.2) ;
- la durée de conservation des données personnelles concernées ;
- la typologie des données collectées et traitées par le sous-traitant pour le compte du responsable du traitement ;
- la catégorie des personnes concernées par la collecte et le ou les traitements ;

1-) GÉNÉRALITÉS SUR LES CONTRATS DE SOUS-TRAITANCE

- les engagements du sous-traitant (article 426) ;

  Ces engagements concernent, entre autres, le niveau de sécurité applicable aux données, le niveau de confidentialité à maintenir sur les données, la publication des mentions d'information ou de collecte du consentement au sein de la solution que le sous-traitant fournit ou administre, ou encore la publication des modalités de collecte du consentement des personnes concernées. Mais c'est bien au responsable de traitement qu'il incombe de les définir et d'exiger cette publication (par exemple, sur son site web ou son application).

- la mise en œuvre et l'entretien d'une documentation précise exposant les mesures de protection et de confidentialité entourant les données ainsi que leurs accès (preuve du niveau de garanties sécuritaires, techniques et organisationnelles offert par la solution du sous-traitant (point 1 al.2 article 386) ;

- l'exigence de coopération entre les parties pour donner effet aux droits des personnes concernées, mais aussi entre les parties et les autorités de contrôle (articles 450, 451 et 483 point 15) ;

- l'assistance entre les parties dans la gestion des demandes des personnes concernées, mais aussi entre les parties et les autorités de contrôle (article 435) ;

- les modalités de notification des violations des données (par le prestataire au client, afin que le client entant responsable du traitement soit en mesure de se conformer à ses propres

obligations et notifie l'APDP à temps, voire les personnes concernées en cas de risque grave sur leurs droits et libertés (article 427)) ;

- les modalités de signalement des demandes des personnes concernées (du prestataire vers le client ou du client vers le prestataire, voire les deux si les demandes des personnes physiques peuvent être adressées aux deux, ce que doit indiquer le contrat. En principe, le prestataire ne répond jamais directement : il relaie la demande au responsable de traitement, seul en mesure de vérifier l'identité du demandeur et la légitimité de sa demande, l'existence d'éventuels motifs de refus, et seul décisionnaire de la réponse à y faire - et des instructions subséquentes à adresser au sous-traitant (articles 416, 418, 419, 420)) ;

- l'entretien de la méthodologie et des procédures internes du prestataire permettant d'attester en tout temps du respect des principes constitutifs de privacy by design et de privacy by default (article 424);

- les mesures d'urgence et palliatives en cas de fuite de données et/ou de non-conformité du dispositif aux niveaux convenus (article 426),

- plus généralement, la tenue à jour de l'ensemble des documents de conformité (accountability (article 387).

1-) GÉNÉRALITÉS SUR LES CONTRATS DE SOUS-TRAITANCE

En pratique, le nombre de thématiques et leur niveau de détail vont varier selon qu'il s'agit d'un contrat entre professionnels ou des conditions d'utilisation d'un service par un consommateur lesquelles relèvent le plus souvent du contrat d'adhésion.

Le plus souvent, l'exposé des mesures techniques de sécurité fera l'objet d'une annexe distincte, ou d'une documentation détaillée qui n'est pas communiquée au client mais qui doit être mise à sa disposition à première demande, toujours dans le cadre de l'accountability.

Enfin, le contrat doit comporter une clause d'audit, permettant au responsable de traitement de « veiller » à ce que le prestataire fournisse bien l'ensemble de ces engagements pendant toute la durée des traitements qui lui sont confiés, jusqu'à la restitution au client et la destruction finale des données en fin de contrat.

Au demeurant, il est très important de comprendre que la conformité ne se limite pas aux contractuels. Les documents contractuels ne peuvent et ne doivent refléter que la réalité des mesures techniques et organisationnelles déployées, sans quoi le prestataire prend des engagements qu'il sait d'emblée ne pas pouvoir tenir.

Le responsable de traitement doit « challenger » les engagements proposés, et comprendre la nature des services qu'il commande.

III°) LA GESTION DE LA PROTECTION DES DONNEES DANS LES RELATIONS CONTRACTUELLES

2-) SPÉCIFICITÉS DE LA SOUS-TRAITANCE DANS LES RAPPORTS DE MARCHÉS PUBLICS

a-) Obligation de respecter le Livre 5ème

Les administrations (État, collectivités territoriales, établissements publics), tout autant que les entreprises privées, sont concernées par la mise en conformité au Livre 5ème.

Ces personnes de droit public peuvent s'appuyer sur des bases légales spécifiques qui justifient leurs traitements, liés souvent aux missions de services publics qui leur sont dévolues (obligations légales ou intérêt généraI).

Mais les obligations leur incombant, en tant que responsable de traitement ou même en tant que sous-traitant, sont les mêmes que celles qui s'imposent aux personnes morales de droit privé.

Il incombe alors au responsable de traitement, fut-il une administration, de prouver que ses intérêts légitimes impérieux prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée. C'est le sens du dernier alinéa de l'article 440 « ...En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d'accès... ».

C'est dire que même lorsque c'est l'administration ou l'État qui collecte des données à caractère personnel, il ne peut s'agir du fait du prince : la mise en balance doit être effectuée entre les objectifs

a-) Obligation de respecter le Livre 5ème

poursuivis par l'administration, d'une part, et la protection des données personnelles et donc des droits et libertés des personnes d'autre part.

Les obligations liées à la sécurité structurelle des outils et services de collecte et traitement de la donnée, l'obligation d'information des droits des personnes concernées, la nécessité d'effectuer des analyses d'impact relatives à la protection des données (AIPD) s'appliquent aux traitements de données personnelles effectués par les personnes publiques, sur les données personnelles de leurs usagers ou administrés. Enfin, la désignation d'un DPO est obligatoire au sein des autorités publiques (article 430).

En tout état de cause, hors législation particulière, dès qu'une entité de droit public passe commande de services ou de solutions traitant de données personnelles, elle est soumise aux principes du Livre et doit gérer, dans le cadre de sa commande publique, la conformité du service ou de la solution cible à cette réglementation.

Pour ce faire, l'acheteur public doit, au moment de recourir à un sous-traitant, s'assurer d'en choisir un qui présente des **«granties suffisantes».**

b-) Réformer les outils contractuels de la commande publique

Les Cahiers des Clauses Administratives Générales (CCAG) sont un outil indispensable aux administrations qui acquièrent des solutions ou services numériques.

Malheureusement, ce document de référence ne comporte pas de clause relative à la protection des données personnelles, ce qui est une lacune évidente. Et désormais, sous l'empire du Code, elle est rédhibitoire.

En l'absence d'une mise à jour des CCAG, les administrations doivent donc y pallier en ajoutant des clauses spécifiques, afin d'attirer l'attention des soumissionnaires sur la nécessaire conformité au Livre 5ème des services, prestations ou plateformes qu'ils proposent en réponse aux appels d'offres de l'administration.

Ces clauses dérogatoires doivent en conséquence figurer dans le cahier des clauses administratives particulières (CCAP) qui constituera, aux côtés du cahier des clauses techniques particulières décrivant les besoins fonctionnels et techniques de l'acheteur, le cœur du marché public.

Il faut souligner que ces exigences s'appliquent quelle que soit la procédure d'achat, quand bien même elle ne serait pas soumise à l'obligation de mise en concurrence.

b-) Réformer les outils contractuels de la commande publique

L'administration est ici le responsable du traitement, et elle doit exiger de celui qui sera son sous-traitant au sens du Livre 5ème qu'il participe pleinement à la conformité des traitements mis en œuvre par l'administration dans le cadre de l'exercice de ses missions de service public ou de l'exécution d'éventuelles activités commerciales accessoires qui seraient les siennes.

Il est préconisé d'insérer dans les documents de la consultation une clause d'exécution qui intègre automatiquement l'engagement contractuel régissant la commande publique, conformément au fonctionnement habituel des marchés publics.

Il faut également indiquer que les documents contractuels qui seraient ajoutés par le candidat ne pourront en aucun cas modifier ou amoindrir les engagements formulés dans les documents de la consultation, conformément là encore aux règles de la commande publique, mais venir compléter et préciser ceux-ci, notamment sur l'ensemble des thématiques suivantes :

- le strict respect par le soumissionnaire des exigences légales et réglementaires en matière de données à caractère personnel, et l'engagement de s'y conformer en tant que sous-traitant, a fortiori si les données sont des données « particulières » (santé, orientations politiques ou religieuses), spécialement attentatoires à la vie privée (difficultés socio-économiques des personnes, condamnations pénales), particulièrement intrusives (données biométriques, génétiques) ou encore relatives à des personnes vulnérables (élèves, personnes âgées, etc.) ;
- l'ensemble des modalités par lesquelles le soumissionnaire entend se conformer aux exigences de la réglementation ;
- le respect des conditions de traitement imposées par le pouvoir adjudicateur (finalités du traitement, durée de conservation, instructions, etc.) ;

b-) Réformer les outils contractuels de la commande publique

- le descriptif de l'infrastructure et des procédures d'exploitation du système du soumissionnaire ;
- la politique de sécurité du soumissionnaire, et notamment la sécurité logique et physique des données personnelles si elles sont appelées à être traitées ou stockées au sein d'une plateforme fournie par ses soins, ou sur son système d'information à l'occasion de l'exécution des services objets de l'appel d'offres ;
- la description par le soumissionnaire de l'ensemble des mesures techniques et organisationnelles pour préserver la sécurité et la confidentialité des données et leur traitement aux seules fins objets de l'appel d'offres ;
- les procédures d'alerte de l'administration responsable de traitement en cas de violation des données sous la responsabilité du candidat ;
- les procédures de relais et d'assistance à l'exécution des demandes des personnes concernées relatives à leurs droits d'accès, de rectification, d'effacement, d'opposition, de limitation, de portabilité, etc., soumises à la décision de l'administration ;
- les modalités d'audit par l'administration, les rapports périodiques à fournir, etc. ;
- la garantie que les données sont hébergées exclusivement sur le territoire de la CEDEAO ;
- les conditions de recours à une sous-traitance ultérieure par le candidat, en exigeant très précisément la désignation et la localisation des sous-traitants ultérieurs, ainsi que la description des traitements qui leur seront spécifiquement sous-traités, sans oublier l'exigence d'autorisation préalable par l'acheteur.

III°) LA GESTION DE LA PROTECTION DES DONNEES DANS LES RELATIONS CONTRACTUELLES

3-) QUID DE L'OFFSHORING ?

La problématique de l'offshoring renvoie à celle des transferts de données et à celle de la légalité du recours aux organismes délocalisés dans des Etats tiers.

D'abord, notons que le Code a voulu s'inscrire dans un cadre communautaire qui faciliterait la libre circulation des données à caractère personnel. Dans ce sens, le Code a vocation à s'appliquer lorsqu'un traitement est effectué au Bénin ou dans un Etat membre de la CEDEAO au sein duquel le principe de libre circulation est établi. Ce sont donc les Etats établis hors de cette Communauté qui sont considérés comme des Etats tiers et soulèvent la problématique d'un transfert encadré des données.

Ces pays n'appliquent pas toujours les mêmes principes de protection des données ou ne disposent tout simplement pas de législation adaptée. Ce qui induit une logique de contrôle accru des opérations de transfert vers eux.

A l'échelle internationale, le contrôle des transferts est réglé soit par :

- Des instruments juridiques spécifiques dont la signature des Clauses Contractuelles Types (CCT) édictées par les autorités européennes et convenant le plus souvent aux contrats entre clients et prestataires notamment en cas d'offshoring ;
- Le déploiement des Règles d'entreprises contraignantes (Biding Corporates Rules -BCR) conclues au sein des groupes de sociétés et régissant les transferts entre filiales et sociétés mères et/ou
- Des mécanismes d'auto-certification dont le Privacy Shield américain qui permet d'attester le niveau élevé d'engagements personnels d'entreprises opérant dans le secteur du traitement des données à caractère personnel.

3-) QUID DE L'OFFSHORING ?

Avec ces outils, les organismes établis hors « zones sûres » parviennent à contracter avec des responsables de traitement de par le monde notamment ceux européens tout en affichant vis-à-vis des autorités de contrôle, un niveau de confiance suffisant pour traiter les données à caractère personnel suivant une orthodoxie généralement partagée et acceptée.

Dans le livre 5ème du Code du numérique, les transferts vers les Etats tiers sont soumis à des exigences similaires qu'à l'international. L'article 391 du Code oblige le responsable de traitement qui compte faire un transfert de données vers un pays tiers ou une organisation internationale **qui n'assure pas « un niveau de protection équivalent à celui mis en place par les dispositions du présent Livre** » à :

Obtenir une autorisation préalable et à

Soumettre le projet de transfert à un contrôle régulier de la finalité du transfert par l'Autorité de Protection des Données à caractère Personnel.

Autrement dit, aucun transfert vers un pays tiers, dans le cadre d'une relation avec une société offshore par exemple, ou une organisation internationale ne peut se faire si ce pays n'offre pas un niveau de protection équivalent à celui mis en place au Bénin.

Dans la lignée du principe de transparence, l'article 391 a indiqué que « Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données… ».

3-) QUID DE L'OFFSHORING ?

A ce titre, l'Autorité est notamment tenue de prendre en compte **l'état du droit et le respect des droits de l'homme et des libertés fondamentales ainsi que l'existence d'une ou plusieurs autorités de contrôle indépendantes dans le pays tiers ou encore de l'existence d'engagement pris par ce dernier ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux.**

A la lueur de ces critères, il s'infère qu'à défaut de niveau équivalent et suffisant de protection dans le pays tiers, les relations contractuelles de l'offshoring peuvent également se nouer en présence d'instruments juridiques contraignants tels que les BCR ou le Privacy Shield.

a-) Le Privacy Shield

Le Privacy Shield est un mécanisme d'auto-certification permettant de transférer les données vers les États-Unis.

Il s'agit d'un mécanisme sectoriel, puisque seules les entreprises relevant de la compétence de la Federal Trade Commission (FTC) ou du Departement of Transportation peuvent adhérer à ce mécanisme.

L'instrument met en place une surveillance proactive trimestrielle par le Département du commerce, avec des contrôles sur place. Il sélectionne de manière aléatoire des sociétés pour vérifier qu'elles respectent les principes du Privacy Shield. Des analyses des sites internet des adhérents au Privacy Shield ont également été mises en place afin de s'assurer que les liens renvoyant vers les politiques de protection de la vie privée sont actifs et corrects.

a-) Le Privacy Shield

En cas d'identification par le Département du commerce d'une entreprise ne respectant pas les principes du Privacy Shield, ce dernier retire alors l'entreprise en cause de la liste des adhérents actifs.

Toutefois, les vérifications mises en place par le Département du commerce ne sont pas suivies d'effets conséquents. Les contrôles réalisés par le Département du commerce n'ont pour l'instant pour objet qu'une simple vérification des formalités réalisées par les entreprises. Ils n'ont à ce stade pas vocation à contrôler véritablement le respect des principes essentiels du Privacy Shield, à savoir notamment le respect du principe de nécessité et de proportionnalité des traitements mis en œuvre.

Plusieurs points ont fait l'objet de critiques ciblées, tels que le traitement des données à des fins ultérieures par les entités importatrices de données aux USA (par exemple, qu'est-ce qu'un membre des GAFAM peut faire des données qu'il collecte dans le cadre des outils de mesure de fréquentation web qu'il propose?).

L'accès des autorités nord-américaines aux données personnelles à des fins de sécurité nationale, et dans le cadre du récent « Cloud Act » pose également problème.

Pour ces raisons notamment, le Privacy Shield demeure un biais fragile pour permettre l'envoi de données à caractère personnel vers le territoire des USA.

En conséquence, il est plus prudent de se fier à des prestataires ou éditeurs américains qui auront déployé des BCR validées au sein de leurs groupes, ou qui auront signé des clauses contractuelles types et déployé les mesures techniques et organisationnelles répondant réellement aux exigences du Code.

b-) Les BCR

Les règles d'entreprises contraignantes (Biding Corporate Rules ou BCR) sont les règles internes relatives aux transferts de données à caractère personnel vers des pays tiers au sein d'un même groupe d'entreprises. Elles constituent le « code de conduite » interne, propre à un groupe d'entreprises, qui définit la stratégie politique en matière de transferts de données pour chacune des entités constituant le groupe, y compris leurs employés.

Elles peuvent aussi être utilisées pour un ensemble d'entreprises qui participent à une activité économique conjointe, mais ne font pas nécessairement partie du même groupe.

Pour une multinationale dont certaines filiales n'auraient pas le niveau équivalent et suffisant de protection des transferts de données, la mise en place de BCR est un choix judicieux pour l'avenir. Au regard de prestataires ou de partenaires, elles permettent d'assurer des garanties appropriées telles que l'application de principes généraux relatifs à la protection des données (limitation de la finalité, minimisation des données, etc.), les droits des personnes concernées, la mise en place d'audits, la constante communication avec l'autorité de contrôle chef de file ou encore la formation du personnel sur les questions de protection des données et ce, pour toutes les entités d'un même groupe. Les BCR représentent un avantage concurrentiel et un atout pour tout contrôle par une autorité de régulation.

b-) Les BCR

Si l'avantage des BCR est indéniable, certaines difficultés peuvent cependant se poser, car les BCR sont un contrat qui lie les parties. Ainsi, chacune des entités d'une multinationale (et désormais même ses sous-traitants s'ils sont inclus au déploiement des BCR) devra elle-même adhérer ou non, totalement ou partiellement, aux BCR du groupe pour qu'elles lui soient applicables.

Privacy Shield, certifications, normalisations, labélisation ou BCR, dans ses relations avec une société offshore présente dans un Etat tiers donc, le responsable de traitement devra arbitrer quant à l'instrument juridique contraignant adéquat en prévision du contrôle de l'opération par l'Autorité.

c-) Sécurité des transferts en cas d'offshoring

Après avoir choisi l'outil le plus adapté pour transférer les données à caractère personnel, le responsable du traitement devra mettre en œuvre une série d'opérations afin de s'assurer de la sécurité de ces transferts et des données transférées.

Afin de se conformer aux exigences du livre notamment à celles de l'article 426 portant sur la sécurité des données à caractère personnel, il est nécessaire de mettre en place une bonne gouvernance juridique.

La gouvernance juridique implique d'identifier les finalités poursuivies, les traitements mis en œuvre,

c-) Sécurité des transferts en cas d'offshoring

les catégories de données transférées, les éventuels destinataires ou sous-traitants ultérieurs, les durées de conservation, etc.

L'identification des éventuels transferts internationaux de données fait partie intégrante de l'inventaire des traitements.

Pour chaque traitement, l'organisation doit, en effet, indiquer les pays vers lesquels les données sont éventuellement transférées, et pour quelle raison.

En particulier, il convient d'auditer ses contrats tout comme son système informatique dès lors que tous les transferts ne sont pas nécessairement couverts contractuellement. Tant les contrats préexistants que ceux en cours de négociations, et identifier les transferts internes et vers les filiales, ceux auprès de sous-traitants, et enfin auprès d'éventuels sous-traitants des sous-traitants.

Les contrats établis ou en cours de négociations avec les sous-traitants ne mentionnent pas toujours les pays de destination du transfert des données.

Le bon réflexe à adopter est alors de rechercher les conditions générales de vente, la politique de protection des données personnelles ou autres mentions légales du prestataire sur son site internet.

Une attention doit également être portée aux contrats conclus entre les sous-traitants et leurs prestataires. Troisième maillon dans la chaîne de responsabilités lorsque le traitement fait l'objet d'un

c-) Sécurité des transferts en cas d'offshoring

transfert à l'étranger, le sous-traitant de second rang est relativement négligé. Plus précisément, le responsable du traitement considère à tort, qu'il appartient au sous-traitant d'encadrer juridiquement et techniquement les éventuels transferts de données à ses propres sous-traitants.

Or, c'est sur le responsable du traitement que le Livre fait peser la sécurisation de l'ensemble de la chaine de sous-traitance. Cependant, seul le prestataire du responsable du traitement pourra véritablement se renseigner directement à la source concernant ses sous-traitants.

Il est donc important de bien répercuter toutes les mesures de sécurité et les obligations contractuelles du contrat avec son prestataire sur celui signé entre le prestataire et son (ou ses) sous-traitant (s).

- Enfin, une fois l'inventaire des transferts achevés, leur existence doit :
  - figurer dans les mentions d'informations (articles 415 et 416) ;
  - faire partir intégrante du registre des traitements tenu par le responsable du traitement (article 435) et
  - être communiquée lors de réponses à une demande d'exercice du droit d'accès (article 437).

Dans le cadre de l'accountability, il appartiendra au responsable du traitement de s'assurer que cet inventaire sera maintenu à jour et que chaque transfert sera bien encadré juridiquement.

Merci !