LE RGPD ET SES IMPLICATIONS DANS LES PAYS HORS UNION EUROPÉENNE

Marguerite OUEDRAOGO / BONANE
PRESIDENTE CIL **BURKINA FASO**

ouedma@gmail.com

Le RGPD est une évolution majeure du cadre juridique de la protection des données personnelles, évolution due entre autres au progrès technologique auquel il tente sans cesse de s'adapter. L'Europe est le précurseur et la locomotive de ce droit. Elle vient de démontrer son rôle prépondérant avec l'entrée en vigueur, le 25 mai 2018, du Règlement général sur la protection des données personnelles (RGPD ou GDPR), plongeant ainsi ses partenaires sociaux et économiques dans une nouvelle réflexion, celle de savoir quelles sont les implications du RGPD pour eux, pays hors Union européenne ?

Pour répondre à cette préoccupation, le plan suivant vous est proposé :

Plan :

- Un aperçu de la législation en matière de PDP ;
- Les principes fondamentaux de la PDP ;
- Un aperçu du RGPD et ses principes fondamentaux ;
- Les implications du RGPD pour les pays hors union européenne.

Aperçu de la législation en matière de protection des données personnelles

En Europe

- La France a été pionnière en Europe quant à la protection des données liées à la société de l'information avec l'adoption de la **loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en août 2004**. D'autres pays d'Europe ont suivi l'exemple français : Belgique, Allemagne, Italie, Suisse, Royaume-Uni, Grèce, Pays-Bas, Portugal, Espagne.

- la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (connue sous le nom de **Convention 108**), adoptée en 1981 par le Conseil de l'Europe est, jusqu'ici, la seule convention à vocation internationale ;

Aperçu de la législation en matière de protection des données personnelles

- la **Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995**, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

- le **Règlement n°2016/679**, dit Règlement général sur la protection des données (**RGPD** ou encore GDPR en anglais, General Data Protection Regulation). Ce texte de l'Union européenne qui constitue aujourd'hui la référence en matière de protection des données à caractère personnel, renforce et unifie la protection des données des personnes.

Aperçu de la législation en matière de protection des données personnelles

Au plan international

L'Assemblée générale des Nations Unies a adopté les principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel, le 14 décembre 1990, dans sa **Résolution 45/95**.

En Afrique

L’effervescence de ce droit a eu comme impact en Afrique deux rencontres préparatoires qui ont été déterminantes ; il s’agit de :

- la rencontre de Bamako de novembre 2000, lors du symposium sur le bilan des pratiques de la démocratie, des droits et libertés dans l’espace francophone, qui a donné naissance à la déclaration, dite de Bamako ;

Aperçu de la législation en matière de protection des données personnelles

- Également, la rencontre de Ouagadougou, à l'occasion de la 9e conférence des chefs d'Etats et de Gouvernements de l'OIF, les 26 et 27 novembre 2004, qui a marqué l'engagement des dirigeants africains à œuvrer pour une protection des données personnelles de leurs citoyens.

- Le Burkina Faso a été le premier pays à adopter une loi sur la protection des données personnelles en Afrique. D'autres pays ont suivi la dynamique : Afrique du Sud, Cap-Vert, Bénin, Côte d'Ivoire, Gabon, Ghana, Guinée Conakry, Niger, Mali, Maroc, Mauritanie, Sénégal, Tchad, Tunisie.

Aperçu de la législation en matière de protection des données personnelles

Au niveau communautaire africain

- **L'acte additionnel A/SA,1/01/10 du 16 février 2010**, relatif à la protection des données à caractère personnel dans l'espace CEDEAO. Cet instrument juridique pose les jalons du droit à la protection des données personnelles et invite chaque Etat à se doter d'une loi et d'une autorité de contrôle.

- **La Convention de l'Union Africaine** sur la sécurité dans le cyberespace et la protection des données à caractère personnel ou **Convention de Malabo, du 27 juin 2014,** qui requiert la ratification de 15 pays africains pour être effective.

L'objet est de **protéger les droits des personnes** en matière de traitements de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables de traitement.

Quelques concepts clés :

- **Donnée à caractère personnel** : toute information qui permet, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques, par réf. à un numéro d'identification ou plusieurs éléments spécifiques propres à leur identité physique, psychologique, psychique, économique, culturelle ou sociale
- **Traitement de données à caractère personnel**
- **Responsable de traitement**
- **Destinataire d'un traitement de données personnelles**
- **Personne concernée.**

L'application du droit à la protection des données personnelles, est basée sur le respect des principes fondamentaux qui se retrouvent dans les législations en la matière. Ce sont :

Les principes fondamentaux du droit à la protection des données personnelles

- le **principe du consentement** : tout traitement de données à caractère personnel doit avoir reçu le **consentement** de la ou des personnes concernées, sauf dérogations prévues par la loi. Outre ce consentement, la personne concernée a le **droit de connaître et de contester les informations et raisonnements** utilisés dans les traitements, automatisés ou non, dont les résultats lui sont opposés et **le droit de s'opposer, pour des raisons légitimes**, à ce que ses données personnelles fassent l'objet de traitement.

- le **principe de la légitimité du traitement** ;
- le **principe de la finalité** ;
- le **principe de sécurité** ;
- le **principe du respect des droits des personnes** (*droit à l'information, droit d'accès, droit de rectification, droit d'opposition, droit à l'oubli*) ;
- le **principe de la proportionnalité et de la pertinence des données collectées** ;
- le **principe de la licéité et de la loyauté de la collecte** ;
- le **principe d'une durée limitée de conservation** des données personnelles ;
- le **principe d'exactitude et de transparence**.

Un aperçu du RGPD et ses 5 principes fondamentaux

Le Règlement général sur la protection des données (**RGPD**) est le nouveau texte de référence européen en matière de protection des données personnelles, pour les résidents de l'Union européenne ; il vise à harmoniser la gestion des données dans l'ensemble des pays de l'Union européenne. Deux constats majeurs ont été à l'origine du RGPD :

- l'inefficacité révélée, en 2012, des lois nationales et communautaires à protéger les données personnelles des citoyens européens ;
- l'affaire SNOWDEN : relative à une surveillance de masse des citoyens européens par les Etats-Unis.

Le RGPD est entré en vigueur le 25 mai 2018.

Le RGPD concerne **tous les acteurs économiques et sociaux proposant des biens et services sur le marché européen**, dès lors que leurs activités traitent des données personnelles des résidents de l'Union Européenne. Seront donc concernés :

- les entreprises ;

- les associations ;

- les organismes publics, mais aussi

- les entreprises dont le siège est hors de l'Union Européenne, mais qui opèrent au sein de l'Union européenne et sur les données des citoyens de l'Union Européenne ; enfin

- les sous-traitants dont les activités entrent dans ce cadre.

L’**objectif** du RGPD est de donner aux citoyens européens d’avantages de contrôle et de visibilité sur leurs données privées, notamment pour savoir quels sont les données personnelles collectées, où sont-elles stockées, à quelles fins, à qui sont-elles transférées et jusqu’à quand ? En un mot, elle vise à garantir le respect des données personnelles et de la vie privée des citoyens européens par tout responsable de traitement, quel que soit le pays d’origine.

Le **principal enjeu** pour les entreprises est de savoir, en un instant donné, où sont les données et comment pouvoir, sur simple demande, les collecter et les transmettre à la personne concernée. Cela suppose que l’entreprise doit connaitre, à tout moment, les données dont elle dispose, leur localisation, l’objectif de leur collecte, leur mode de gestion, de stockage, de transfert et d’effacement.

Afin d’inciter les entreprises à s’y engager sérieusement, il est prévu des sanctions en cas de non-conformité au RGPD qui vont de :

- 2 à 4% du chiffre d’affaires mondial des entreprises, ou de

- 10 à 20 millions d’euros.

Dans tous les cas, c’est la somme la plus importante qui sera retenue et il reviendra à

Présentation brève du RGPD et ses 5 principes fondamentaux

Le RGPD contient **5 principes majeurs** :

- l'**Accountabililty** qui introduit une logique de responsabilisation selon lequel, il revient à l'entreprise de prendre toutes les dispositions pour garantir sa conformité au RGPD et démontrer à l'Autorité de contrôle dont elle relève qu'elle a rempli ses obligations ;
- la démarche de **Privacy by design** signifie que la protection des données personnelles est prise en compte dès la conception du produit ou du service, notamment dans le système d'informations de l'entreprise, au sein d'une base de données, ou lors de la conception d'une application ;
- le principe de **Security by default** ou la sécurité par défaut consiste à renforcer le rôle de la sécurité dans le système d'information. En effet, le système d'information de l'entreprise doit être sécurisé à tous les niveaux, du physique au logique, avec par exemple, des contrôles d'accès ou des systèmes de prévention contre les failles éventuelles de sécurité ; l'entreprise doit être à mesure de déceler si son système d'information a été compromis et pouvoir y remédier en un temps record. Pour cela, elle doit limiter l'accès aux DP, éviter les copies multiples et minimiser les données stockées.

Présentation brève du RGPD et ses 5 principes fondamentaux

- la désignation d'un **Data Protection Officer** (DPO) ou délégué à la protection des données personnelles.

Le DPO doit être associé aux différentes questions et problématiques de protection des données à caractère personnel de l'entreprise ; son rôle est de veiller à la conformité au RGPD des traitements effectués et d'être le point de contact avec les Autorités de contrôle.

Le profil du DPO varie selon les entreprises.

- la réalisation d'une **étude d'impact** : le RGPD recommande aux entreprises de réaliser une étude d'impact avant la mise en œuvre de nouveaux traitements de données personnelles, qui pourraient potentiellement présenter des risques d'atteinte aux droits et aux libertés individuelles.

Il convient de relever que le RGPD vient engager davantage la responsabilité des responsables de traitement et celle des sous traitants, renforcer les droits des personnes concernées, renforcer les sanctions pour non conformité.

Les implications pour les pays hors union européenne

Si le RGPD a tant défrayé la chronique, c'est à cause de son **applicabilité extraterritoriale** (hors UE). En effet, il s'adresse à tous les pays du monde et vise à contraindre les géants du Net que sont les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), au respect des données personnelles des internautes.

L'article 3 du RGPD précise que le Règlement s'applique aux traitements des données effectués dans le cadre **des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.**

Le RGPD s'applique au **traitement des données personnelles relatives à des personnes concernées qui se trouvent sur le territoire de l'Union**, par un responsable de traitement ou un sous-traitant qui n'y est pas établi, lorsque les activités sont liées à l'**offre de biens ou de services à ces personnes concernées dans l'Union ;**

Les implications pour les pays hors union européenne

Également **il s'applique au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.**

Exemple, quand un web entrepreneur suit le comportement des citoyens résidents au sein de l'Union à des fins publicitaires ou de profilage, il doit se conformer au RGPD.

En ce qui concerne les offres de biens et services et le suivi du comportement, l'article 27 du RGPD exige **la désignation par l'entreprise d'un représentant** dans l'Union.

Pour ce qui est **des transferts de données hors Union européenne**, le RGPD exige un **niveau de protection adéquat** dans le pays destinataire et à défaut, des garanties appropriées ou l'application de règles contraignantes par les groupes d'entreprises impliquées.

Les implications pour les pays hors union européenne

En résumé, une lourde sanction peut être infligée aux entreprises hors de l'Union, qui ne se conforment pas au RGPD. Cela peut arriver à une entreprise africaine établie hors de l'Union, qui a un représentant qui opère au sein de l'Union et qui ne se conforme pas au règlement.

Il peut lui être adressé un avertissement, ou il peut être indexé comme étant une entreprise non respectueuse des données personnelles, situation de nature à ternir son image.

Les implications pour les pays hors union européenne

Le RGPD a d'autres effets qui consistent en la protection des droits des personnes hors UE, notamment face aux actions des géants du Net, par l'application du droit à l'oubli.

Le principe du privacy by design : devra être pris en compte par les entreprises hors UE dans leur processus de production de biens et services pour être compétitives sur les marchés européens, et résister ou faire face à la concurrence.

Point des actions menées par la CIL dans le cadre de l'entrée en vigueur du RGPD

- Publication d'article dans la presse écrite et en ligne , de même que sur le site web de la CIL.
- Intervention de Mme la Présidente sur le Plateau du JT de Burkina Info.
- Diffusion de communiqués, dans leFaso.net, sur le site de la CIL et bande défilante sur Burkina Info.

Séminaire international des cadres des autorités de Protection des données personnelles du 10 au 11 juillet 2018 :

- réalisation et diffusion de spot télé en français et en langues nationales ;
- réalisation er diffusion de spot radio en français et en langues nationales.

La CIL lors de la relecture de la loi sur la protection des données personnelles a pris en compte les exigences du RGPD, notamment par :
- la désignation du délégué à la protection des données personnelles ;
- le renforcement des droits des personnes par la prise en compte du droit à l'oubli ;
- le renforcement des sanctions à administrer .

Quant à l'obligation d'assurer la sécurité des données par des mesures techniques et organisationnelles, la question n'est pas nouvelle et a toujours été évoquée lors de nos actions de sensibilisation. Aussi, la CIL a déjà initié un atelier de formation au profit des Webmasters, des gestionnaires de sites web public/privé afin qu'ils prennent en compte de la protection des données personnelles dès la conception de leurs produits.

Relativement à l'étude d'impact, la CIL accompagne les entreprises par des conseils et recommandations, soit à l'occasion de l'accomplissement des formalités préalables, soit lors de ses missions de contrôle sur le terrain.

Conclusion

Il faut retenir que le nouveau règlement impacte les entreprises aussi bien à l'intérieur qu'à l'extérieur de l'Union européenne. En somme, toute entreprise qui gère des données de résidents ou d'entreprises européennes, devra se conformer au RGPD.

Les pays africains, notamment au sein du Réseau africain des autorités de protection des données personnelles (RAPDP), s'activent afin de revoir, à terme, leurs législations pour mieux protéger les droits et libertés fondamentaux de leurs citoyens.

Je vous remercie pour votre attention !