Brève analyse de la loi togolaise relative à la protection des données à caractère personnel

Dessa-Nin Ewèdew Awesso

BRÈVE ANALYSE DE LA LOI TOGOLAISE RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Dessa-nin Ewèdew Awesso
Doctorant en Cotutelle
Université Côte d'Azur/Université de Lomé

Après l'adoption de la loi relative à la cybersécurité et la lutte contre la cybercriminalité[1], le Togo fait un pas de plus dans la gestion des risques et menaces liés aux activités numériques. En effet, c'est par la loi du 29 octobre 2019 relative à la protection des données à caractère personnel[2] (LPDCP) que le Togo compte réglementer la collecte, le traitement, la transmission, le stockage, l'usage et la protection des données à caractère personnel.

Le texte adopté a pour objectif de garantir que tout traitement de données à caractère personnel, sous quelque forme que ce soit, ne porte atteinte aux libertés et aux droits fondamentaux des personnes physiques[3]. Par cette loi, le législateur togolais emboîte notamment le pas du Bénin[4], du Burkina-Faso[5], de la Côte d'ivoire[6], du Ghana[7], du Maroc[8], du Niger[9], du Sénégal[10], ou encore plus récemment du Congo pour ne citer que ceux-là.

Toutefois il s'agit surtout d'une mise en conformité avec la législation communautaire, principalement de l'Acte additionnel relatif à la protection des données à caractère personnel dans l'espace CEDEAO adopté en 2010[11]. Il en est de même avec la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel adoptée en 2014.

---

[1] Loi n° 2018-062 du 7 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité.
[2] Loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel, *JO*, 64e Année N° 26 ter, Numéro spécial, 29 octobre 2019, pp. 1-20.
[3] Article 1er de la LPDCP.
[4] Loi n° 2009-09 du 27 avril 2009 portant protection des données à caractère personnel en République du Bénin.
[5] Loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel.
[6] Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.
[7] *Data Protection Act*, 2012 (*Act* 843).
[8] Loi n° 09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
[9] Loi n° 2017-28 du 03 mai 2017 relative à la protection des données à caractère personnel.
[10] Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel.
[11] Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO du 16 Février 2010. Cet acte additionnel semble avoir été influencé par 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, *JO*, n° L 281, 23/11/1995, pp. 31-50.

En effet, l'Acte additionnel de la CEDEAO dispose en son article 2 que *« chaque État membre met en place un cadre légal de protection de la vie privée et professionnelle consécutive à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel sous réserve de la protection de l'ordre public »*. Quant à la Convention de l'Union africaine, elle dispose en son article 8.1 que *« chaque État partie s'engage à mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel »*.

Si on ajoute à ces textes juridiques, le règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD)[12], on peut considérer – surtout au regard de son contenu – que ladite loi est une vraie-fausse révolution.

Néanmoins, et même s'il a fallu près de dix ans au législateur togolais pour se mettre au diapason de la législation communautaire, la LPDCP a quand même le mérite de s'être largement inspiré des évolutions récentes en matière de protection des données personnelles notamment du règlement européen de 2016 relatif à la protection des données à caractère personnel.

L'entrée en vigueur de cette loi, qui vise à garantir une meilleure protection des données personnelles, aura un impact non négligeable dans l'environnement numérique togolais qui ne semble pas encore y être préparé même si le vent d'une telle réforme soufflait depuis 2010 avec l'Acte additionnel de la CEDEAO.

En outre, il convient de rappeler que cette loi s'applique sans préjudice, entre autres, des dispositions de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, ou encore du décret n° 2018-109/PR portant autorisation de la mise en œuvre d'un traitement autorisé de données à caractère personnel pour l'intégration des grands facturiers à la plateforme électronique de partage des informations sur le crédit.

---

[12] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JO*, n° L119, 4 mai 2016, pp. 1-88.

Sans prétendre à l'exhaustivité, nous nous intéresserons particulièrement au cadre juridique instauré (I) puis à la garantie du respect de la loi relative à la protection des données à caractère personnel (II).

I. Le cadre juridique

L'analyse du cadre juridique de la LPDCP conduit à étudier à son champ d'application (A) et les prescriptions que cette loi met à la charge des personnes procédant au traitement des données à caractère personnel (B).

A. Le champ d'application

Nous étudierons tour à tour le champ d'application *ratione materiae* (1) – en fonction de l'objet – le champ d'application *ratione loci* (2) – en fonction du lieu – et le champ d'application *ratione personae* (3) – en fonction de la personne – de la loi relative à la protection des données à caractère personnel.

1. Le champ d'application *ratione materiae*

Aux termes de son article 4, la LPDCP définit les données à caractère personnel comme étant *« toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique »*[13].

Sont donc d'emblée exclues, du champ d'application de ladite loi, les données relatives aux personnes morales. Par ailleurs, sont exclus les traitements de données mis en œuvre par des personnes physiques dans le cadre exclusif de leurs activités personnelles ou domestiques, à condition que les données ne soient pas communiquées systématiquement à des tiers ou diffusées[14].

Il en est de même pour les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, et à seule fin de permettre à

[13] Voir également l'article 1er de l'Acte additionnel de la CEDEAO.
[14] Article 3.1 de la LPDCP.

d'autres destinataires du service le meilleur accès possible aux informations transmises[15]. Il convient de relever que ce cas exclusion n'était pas prévu par l'acte additionnel de la CEDEAO de 2010[16].

S'agissant du traitement des données à caractère personnel qui est au cœur de la loi, il s'agit de toute opération ou ensemble d'opérations[17] effectuées ou non à l'aide de procédés automatisés telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction des données personnelles[18]. Le choix d'une énumération non limitative des modes de traitement permet au législateur d'englober les nouvelles formes de traitement qui pourraient apparaître. Qu'en est-il du champ territorial de la loi relative à la protection des données à caractère personnel ?

2. Le champ d'application *ratione loci*

Selon les dispositions de l'article 2.3 de la LPDCP, cette dernière s'applique à tout traitement mis en œuvre sur le territoire de la République togolaise ou en tout lieu où la loi togolaise s'applique. Il en est de même pour tout traitement mis en œuvre par un responsable, établi ou non sur le territoire de la République togolaise, qui recourt à des moyens de traitement situés sur le territoire togolais, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit[19].

La notion de moyens doit être ici entendue au sens large c'est-à-dire aussi bien sur le plan humain que technique : le recours à un sondage, à un sous-traitant ou encore à des *cookies*[20]. Il en est ainsi indépendamment du fait que le responsable du traitement – ou son sous-traitant – soit ou non établi sur ledit territoire.

---

[15] Article 3.2 de la LPDCP. Voir également l'article 9 de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.
[16] Article 4 de l'Acte additionnel de la CEDEAO.
[17] Prévues à l'article 2 de ladite loi.
[18] Article 4 alinéa 20 de la loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel.
[19] Article 2.4 de la LPDCP.
[20] Informations, échangé entre le serveur d'un site web et l'ordinateur d'un utilisateur connecté à Internet, permettant au serveur d'un site visité de récupérer des données d'ordre statistique sur sa fréquentation.

Outre le critère d'établissement – et de moyens – on aurait pu espérer que la LPDCP introduise expressément, à l'instar du législateur européen, un critère tourné vers la personne concernée par le traitement[21]. L'objectif étant celui d'appliquer la loi dès lors que les personnes concernées se trouvent au Togo, même lorsque le responsable du traitement n'est pas établi au Togo voire dans la CEDEAO, et que le traitement est lié à l'offre de biens ou de services – gratuits ou onéreux – à ces personnes ou au suivi de leur comportement[22]. Il s'agit du critère de ciblage des personnes concernées. Ce dernier n'était pas non plus prévu par l'Acte additionnel de la CEDEAO[23].

En effet, l'offre de biens et services peut se déduire de l'utilisation de la langue ou de la monnaie d'usage avec la possibilité de passer des commandes dans cette langue[24]. Quant au suivi comportemental, il peut s'agir du suivi du comportement sur internet en vue d'un profilage[25]. De ce fait, l'usage par exemple de *cookies* pour suivre le comportement des internautes dans le but, notamment, de faire du ciblage publicitaire serait ainsi expressément pris en compte. Une telle démarche vise principalement le commerce électronique quelque soit le lieu de situation des entreprises. Le cas où aucun établissement ni moyen ne se trouvent sur le territoire togolais mais qu'une activité est dirigée vers ledit territoire serait alors expressément couvert[26].

En ce qui concerne le transfert des données à caractère personnel vers un pays tiers[27], celui-ci n'est autorisé que sous réserve de réciprocité et si cet État assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes concernées par le traitement. Pour s'assurer d'un traitement adéquat des données, les responsables de traitement peuvent conclure un contrat de transfert, garantissant une protection maximale des données, ou encore adopter des règles d'entreprises contraignantes (en anglais *Binding Corporate Rules ou BCR*)[28] dans le cadre des groupes de sociétés.

---

[21] Voir en ce sens P. Cadio et Th. Livenais, « Photographie du champ territorial du règlement données personnelles : de nouveaux opérateurs concernés ? », *Dalloz IP/IT*, juillet-août 2016, p. 347 et s.
[22] Voir article 3.2 du RGPD.
[23] Voir article 3.3 de l'Acte additionnel de la CEDEAO.
[24] Considérant 23 du RGPD.
[25] Considérant 24 du RGPD.
[26] Voir P. Cadio et Th. Livenais, précité.
[27] Voir article 29 de la LPDCP.
[28] Les règles d'entreprise contraignantes (BCR) sont définies à l'article 47 du RGPD. Elles désignent une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. Elles sont juridiquement contraignantes et respectées par les entités signataires du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés d'une même entreprise ou d'un même groupe.

Dans le cas des contrats de transfert des données personnelles vers des pays tiers, la Commission européenne a prévu des clauses contractuelles types considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes[29]. S'agissant des BCR, qui ont entre autres comme avantage d'éviter de conclure autant de contrats qu'il existe de transferts au sein d'un groupe, on pourrait les classer en deux catégories. D'une part, les BCR « responsable de traitement » encadrant les transferts effectués au sein d'un groupe agissant en qualité de responsable de traitement ; et d'autre part, les BCR « sous-traitant » permettant d'assurer la sécurité des transferts effectués lorsque le groupe agit en qualité de sous-traitant[30].

Selon LPDCP, avant tout transfert des données à caractère personnel du Togo vers un pays tiers, le responsable du traitement doit préalablement informer l'Autorité de protection des données à caractère personnel[31]. Cependant, des transferts ponctuels des données personnelles vers des pays ne répondant pas aux conditions précitées sont autorisées à condition que le transfert ne soit pas massif et que la personne concernée y ait expressément consenti[32]. Reste encore à définir ce qu'il faudrait entendre par transfert « non massif ».

Le transfert ponctuel est possible s'il s'avère nécessaire notamment : à la sauvegarde de la vie de la personne concernée ; au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ; à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci.

En outre, l'Autorité de protection peut autoriser le transfert vers un pays tiers n'assurant pas un niveau de protection adéquat lorsque le responsable du traitement offre des garanties

---

[29] Voir en ce sens la décision (modifiée) de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, *JO,* n° L 39, 12.2.2010, pp. 5-18. Voir aussi la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 modifiant les décisions 2001/497/CE et 2010/87/UE relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers et vers des sous-traitants établis dans ces pays, en vertu de la directive 95/46/CE du Parlement européen et du Conseil, *JO,* n° L 344, 17.12.2016, pp. 100-101.

[30] Selon les activités qu'il souhaite encadrer, le groupe peut opter pour l'un ou l'autre. Toutefois, il est également possible de les adopter concurremment. Voir en ce sens CNIL, « Les règles d'entreprise contraignantes (BCR - Binding Corporate Rules) », 05 septembre 2018, disponible en ligne : https://www.cnil.fr/fr/les-regles-dentreprise-contraignantes-bcr-binding-corporate-rules.

[31] Article 28 de la LPDCP. Aux termes de l'article 1er, alinéa 1, de l'Acte additionnel de la CEDEAO, il s'agit de l'autorité nationale administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions légales.

[32] Article 29 de la LPDCP.

suffisantes[33]. L'Autorité doit également vérifier si le responsable du traitement au Togo offre des garanties suffisantes lorsque les données à caractère personnel proviennent de l'étranger[34].

Il convient de rappeler que dans le cadre de la protection des données personnelles, la LPDCP sera confrontée à l'extraterritorialité de certaines lois. En effet, les GAFAM[35], qui ont une position dominante dans le domaine du numérique, sont soumis à la législation américaine notamment le *patriot act*[36] et le *cloud act*[37]. Ces lois créent des accès aux données, de citoyens américains ou non, stockées par ces entreprises au profit de l'administration américaine.

Le *patriot act* donne autorité aux agences gouvernementales américaines pour accéder aux données en possession des entreprises américaines – quel que soit le lieu où elles sont stockées – dans le cadre de la lutte contre le terrorisme. En pratique, les services de sécurité peuvent ainsi avoir accès aux données détenues par les particuliers et les entreprises – à l'instar des GAFAM – sans autorisation ou information préalable de la personne concernée.

En outre, le *cloud act* permet aux autorités américaines bénéficiant d'un mandat d'avoir accès aux données électroniques stockées par toute société de droit américain dans le cadre d'enquêtes judiciaires. Il a pour objectif de faciliter l'accès aux données en s'adressant directement aux fournisseurs *cloud* plutôt que d'utiliser une demande d'entraide judiciaire qui est une procédure parfois assez longue.

Ainsi les données personnelles concernant des citoyens togolais stockées par des fournisseurs américains peuvent être transmises aux autorités judiciaires américaines s'ils sont suspectés dans une enquête judiciaire et qu'un mandat a été formulé contre eux. Il importe peu que les données soient localisées sur des serveurs hors du territoire américain, seul est pertinent la nationalité de l'entreprise qui détient les données.

Si l'espace territorial concerné par la LPDCP est circonscrit, il revient également de s'interroger sur l'identité des personnes qui y sont soumises.

---

[33] Article 30 de la LPDCP.
[34] Article 31 de la LPDCP.
[35] Google, Apple, Facebook, Amazon et Microsoft.
[36] *Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Public Law 107-56.*
[37] *Clarifying Lawful Overseas Use of Data Act of 2018 (CLOUD ACT), Public Law 115-141.*

3. Le champ d'application *ratione personae*

Aux termes de l'article 2.1 de la LPDCP, la loi s'applique, entre autres, à toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé. Ces derniers sont désignés comme étant les responsables de traitement[38]. La loi ne fait donc pas de distinction entre le fait qu'il s'agisse de personnes physiques ou morales, privées ou publiques.

Sont également soumis au respect de ladite loi les sous-traitants. Ce sont des personnes physiques ou morales, publiques ou privées, tout organisme ou association qui traite des données pour le compte du responsable du traitement[39]. Toute la chaîne de traitement des données est ainsi prise en compte.

Enfin, les personnes concernées désignent toute personne physique qui fait l'objet d'un traitement des données à caractère personnel[40]. *Quid* alors des impératifs légaux que devront respecter les responsables de traitement dans le cadre de leurs activités et spécifiquement dans le cadre de la protection des données personnelles ?

B. Les prescriptions légales

Les responsables de traitement – et leurs sous-traitants – sont, à certaines conditions, soumis à l'accomplissement de certaines formalités préalables (1). Outre ces formalités, des règles encadrant l'activité proprement dite doivent également être respectées (2).

1. Les formalités préalables au traitement

L'exécution de certaines formalités est nécessaire avant de procéder au traitement des données à caractère personnel. Néanmoins, certains traitements sont dispensés des formalités préalables[41]. Il s'agit notamment : des traitements visant la tenue d'un registre destiné à l'information du public et ouvert à la consultation ; des traitements pour lesquels le responsable du traitement a désigné un correspondant à la protection des données à caractère personnel sauf

[38] Article 4 alinéa 16 de la LPDCP.
[39] Article 4 alinéa 17 de la LPDCP.
[40] Article 4 alinéa 14 de la LPDCP.
[41] Voir article 5 de la LPDCP.

lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers est envisagé. Dans ce dernier cas, le responsable du traitement doit en informer l'IPDCP qui donne un avis motivé[42]. Les autres traitements sont soit soumis au régime de la déclaration, soit au régime de l'autorisation, soit au régime de la demande d'avis.

Selon la LPDCP, relèvent du régime de la déclaration les traitements qui ne sont ni dispensés des formalités préalables, ni soumis à une autorisation préalable, ni soumis à une demande d'avis préalable[43]. Cependant, seule la réception du récépissé de déclaration donne droit à la mise en œuvre d'un traitement[44]. Toutefois, l'article 7 de la LPDCP exonère de l'obligation de déclaration les catégories les plus courantes de traitement des données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés. La procédure peut être aussi seulement simplifiée.

En revanche, sont soumis au régime de l'autorisation les traitements portant sur : les données génétiques et sur la recherche dans le domaine de la santé ; les données relatives aux infractions, condamnations ou mesures de sûreté ; les données personnelles ayant pour objet l'interconnexion de fichiers[45], les données portant sur un numéro national d'identification ou tout autre identifiant de portée générale ; les données biométriques et les traitements ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques[46].

Enfin, sont soumis à une obligation de demande d'avis les traitements relatifs : à la sûreté de l'État, la défense ou la sécurité publique ; à la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ; au recensement de la population ; aux données faisant apparaître les origines raciales, ethniques, la filiation, les opinions politiques, philosophiques, ou religieuses ou l'appartenance

[42] Article 28, alinéa 2, de la LPDCP.
[43] En France, la nouvelle loi (Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles , *JO*, 21 juin 2018, texte n° 1) supprime l'intégralité des dispositions de la Loi Informatique et Libertés (LIL) de 1978 qui imposaient une déclaration préalable à la mise en œuvre du traitement.
[44] Article 5, alinéa 2, de la LPDCP.
[45] Voir article 33 de la LPDCP.
[46] Article 8 de la LPDCP. Voir également l'article 12 de l'Acte additionnel de la CEDEAO.

syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci[47] ; au traitement de salaires, pensions, impôts, taxes et autres liquidations[48].

Il s'agit de traitements automatisés d'informations nominatives – opérés pour le compte de l'État, d'un Établissement public, d'une collectivité locale ou d'une personne morale de droit privé gérant un service public – qui outre le cas où ils doivent être autorisés par la loi, doivent en plus être décidés par un acte réglementaire après avis motivé de l'Autorité de protection.

Par ailleurs, la LPDCP soumet l'interconnexion des fichiers relevant de personnes morales gérant un service public à l'obtention préalable d'une autorisation. Il en est de même pour les traitements mis en œuvre par l'État aux fins de mettre à la disposition des administrés des services à distance. Les personnes privées sont également tributaires d'une telle obligation[49].

Qu'ils soient ou non soumis à une formalité préalable, le traitement des données à caractère personnel proprement dit obéit à un ensemble de principes d'où sont déduites des obligations mises à la charge des responsables du traitement.

2. L'encadrement du traitement proprement dit

Le législateur a énuméré sept principes de bases devant soutenir le traitement des données à caractère personnel : le principe du consentement et de légitimité ; le principe de licéité et de loyauté ; le principe de finalité, de pertinence et de conservation ; le principe d'exactitude ; le principe de transparence ; le principe de confidentialité et de sécurité ; du principe du choix du sous-traitant[50]. On peut y ajouter les principes de base de traitement des données sensibles[51].

L'encadrement des traitements des données à caractère personnel varie selon la catégorie à laquelle elles appartiennent. Ainsi, le traitement des données sensibles est par principe interdit[52]. Sont ainsi concernées, *« toutes les données à caractère personnel relatives à l'origine raciale ou éthique, aux opinions ou activités religieuses, philosophiques, politiques, syndicales,*

---

[47] Lorsqu'une interconnexion n'est pas envisagée ou toute autre forme de mise en relation. Voir l'article 10.3 de la LPDCP.
[48] Article 9, alinéa 2, de la LPDCP.
[49] Voir article 32 et suivants de la LPDCP.
[50] Voir les articles 14 à 20 de la LPDCP.
[51] Voir article 21 et suivants de la LPDCP.
[52] Article 21 de la LPDCP.

à la vie sexuelle, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives »[53].

Toutefois, cette interdiction ne s'applique pas lorsque par exemple : le traitement porte sur des données manifestement rendues publiques par la personne concernée ; la personne concernée a donné son consentement par écrit à un tel traitement et en conformité avec les textes en vigueur ; le traitement des données est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ; le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice[54].

En outre, les données relatives aux infractions ne peuvent être traitées que par : les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ; les auxiliaires de justice pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi[55].

Quant aux données de santé, le traitement n'est admis que lorsque entre autres : la personne concernée a donné son consentement ; les données sont manifestement rendues publiques par la personne concernée ; cela est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'autre personne dans le cas où celle-ci ne peut donner son consentement ; cela est nécessaire aux fins de médecine préventive de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à son parent ou lorsque les services de santé agissent dans l'intérêt de la personne concernée[56].

La LPDCP encadre aussi l'utilisation des traitements algorithmiques dans la prise de décisions. Ainsi, l'article 27 de la LPDCP dispose qu'aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour seul fondement un traitement automatisé des données personnelles destiné à évaluer certains aspects de sa personnalité. De même, aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé.

---

[53] Article 4, alinéa 8, de la LPDCP.
[54] Article 22 de la LPDCP.
[55] Article 23 de la LPDCP.
[56] Article 24 de la LPDCP.

Toutefois, sont considérées comme n'étant pas prises sur le seul fondement d'un traitement automatisé des données personnelles : les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations ni celles satisfaisant les demandes de la personne concernée par le traitement[57].

La LPDCP reconnaît également des droits aux personnes concernées par le traitement. Il s'agit : du droit à l'information ; du droit d'accès du droit d'opposition ; du droit de rectification et de suppression ; du droit à l'effacement ; de la sauvegarde des données à caractère personnel après la mort[58]. En outre, pour assurer le respect des droits des personnes concernées, le législateur fait peser sur le responsable du traitement : l'obligation de confidentialité ; l'obligation de sécurité ; l'obligation de conservation ; l'obligation de pérennité[59].

Afin de garantir le respect du cadre juridique de la loi relative à la protection des données à caractère personnelle, le législateur a prévu des garde-fous censés à la fois dissuader, et punir tout manquement, mais également rassurer les personnes concernées par les traitements quant à la sauvegarde de leurs libertés et droits fondamentaux.

II. La garantie du respect du cadre juridique

C'est par le biais d'un contrôle et d'une surveillance renforcée (A) et l'édiction de sanctions à vocation dissuasive et punitive (B) que le législateur espère assurer le respect de la loi relative à la protection des données à caractère personnel.

A. Le contrôle

En matière de protection des données personnelles, on assiste à un contrôle à double détente : un contrôle externe (1) et un contrôle interne (2) du traitement effectué par les responsables de traitement.

[57] Article 27, alinéa 3, de la LPDCP.
[58] Voir article 35 et suivants de la LPDCP.
[59] Articles 51 à 24 de la LPDCP.

1. Le contrôle externe

Pour assurer son pouvoir de contrôle sur les activités de traitement des données à caractère personnel, les pouvoirs publics ont prévu, conformément à l'Acte additionnel de la CEDEAO[60], et à la Convention de l'Union africaine[61], la création de l'Instance de Protection des Données à Caractère Personnel (IPDCP)[62].

Cette institution est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi. Elle a également pour mission d'informer aussi bien les responsables de traitement que les personnes concernées de leurs droits et obligations.

Parmi les missions de l'IPDCP figurent entre autres : l'information du procureur de la République des infractions dont elle a connaissance ; la prise de sanctions à l'égard d'un responsable de traitement ; le conseil des personnes et organismes ayant recours aux traitements des données personnelles ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements[63]. Aux termes de l'article 13 de la LPDCP, l'instance de protection des données à caractère personnel peut être saisie par toute personne agissant pour son propre compte ou une personne physique ou morale dûment mandatée.

Dans le cadre de leur mission de contrôle, les membres du comité de direction de l'IPDCP et les agents peuvent demander la communication de tous documents nécessaires à l'accomplissement de leur mission. Ils peuvent aussi accéder aux programmes informatiques et aux données, demander la transcription de tout traitement dans des documents appropriés directement utilisables pour les besoins du contrôle[64]. Les membres de l'IPDCP et les agents assermentés peuvent également faire des perquisitions – dans les conditions prévues par les articles 75 et suivants du Code de procédure pénale – à condition d'en avoir préalablement informé le procureur de la République[65].

---

[60] Voir article 14 et suivants de l'Acte additionnel de la CEDEAO.
[61] Voir article 11 et suivants de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel.
[62] Article 55 de la LPDCP.
[63] Voir l'article 56 de la LPDCP.
[64] Article 68 de la LPDCP.
[65] Article 66 de la LPDCP.

En dehors du contrôle effectué par l'Autorité de protection, il est également du devoir des responsables de traitement d'organiser un contrôle interne des traitements des données à caractère personnel auxquels ils procèdent.

2. Le contrôle interne

Avec l'adoption de la LPDCP, le contrôle en matière de protection des données à caractère personnel est aussi interne aux structures responsables des traitements. Ce rôle sera assuré par un *« correspondant à la protection des données à caractère personnel »*[66]. Il s'agit d'une innovation du législateur togolais, par rapport au législateur communautaire qui n'avait prévu qu'un contrôle externe – effectué par l'Autorité de protection – dans l'Acte additionnel de 2010. La Convention de l'Union africaine de 2014 ne l'avait pas non plus prévue. La LPDCP marche ici dans l'ombre de la Loi française Informatiques et Libertés de 1978 modifiée en 2018 après l'entrée en vigueur du RGPD[67].

La mission du correspondant à la protection des données à caractère personnel est celle entre autres : d'informer et conseiller le responsable du traitement et le sous-traitant ainsi que les employés quant à leurs obligations légales ; de veiller au respect des dispositions légales en matière de protection des données personnelles ; de donner des conseils sur demande en ce qui concerne l'analyse d'impact relatif à la protection des données à caractère personnel (AIPDCP) ; de coopérer avec l'Autorité de protection ; de faire office de point de contact avec l'Autorité de protection sur les questions relatives au traitement[68].

Il convient de rappeler que l'AIPDCP est un outil important pour la responsabilisation des organismes en les aidant non seulement à mettre en place des mécanismes de traitements protecteur des données à caractère personnel, mais aussi à démontrer leur conformité aux dispositions légales. Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées. L'AIPDCP doit être menée avant la mise en œuvre du traitement et mise à jour tout au long de son cycle de vie. Cependant, en l'absence de précisions suffisantes dans la LPDCP – et en l'absence de prévision dans le

[66] Voir article 75 de la LPDCP.
[67] Voir l'article 37 du RGPD.
[68] Article 76 à 78 de la LPDCP.

cadre de l'Acte additionnel de la CEDEAO – il faudra donc attendre que le cadre de mise en œuvre de l'AIPDCP soit défini par l'IPDCP[69].

En outre, en tant que point de contact, le correspondant doit faciliter l'accès aux documents et informations dans le cadre par exemple d'échanges avec l'Autorité de protection dans l'instruction d'une plainte ou encore dans le cadre d'un contrôle. En outre, l'obligation de secret professionnel du correspondant ne peut l'empêcher de demander conseil à l'IPDCP sur toute question concernant les activités de l'organisme qui l'emploie.

Aux termes de l'article 75, alinéa 1er, de la LPDCP, le correspondant est *« une personne bénéficiant des qualifications requises pour exercer les missions définies »*. L'article 37 du RGPD précise que ce dernier est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

A priori, il peut s'agir d'une personne physique ou d'une personne morale. Ainsi, une personne morale peut être désignée comme étant un correspondant à la protection des données à caractère personnel dès lors qu'elle est susceptible de répondre aux charges qui lui sont imposées. Par ailleurs, puisqu'il est de la compétence de l'IPDCP de définir le profil du correspondant à la protection des données à caractère personnel[70], il lui reviendra alors de dire si une personne morale externe à la structure – à l'instar d'un cabinet de conseil – pourrait ou non jouer ce rôle.

La présence d'une telle personne auprès d'un responsable de traitement – ou son sous-traitant – a donc pour effet de permettre et d'aider l'entreprise à s'autoréguler voire, le cas échéant, à s'autocensurer. Le correspondant bénéficie à ce titre d'une certaine immunité dans la mesure où il ne peut faire l'objet d'aucune sanction de la part de son employeur du fait de

[69] À titre d'exemple, en France une analyse d'impact doit être menée, soit lorsque le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de la réaliser, soit lorsque le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29 : évaluation/*scoring* (y compris le profilage) ; décision automatique avec effet légal ou similaire ; surveillance systématique ; collecte de données sensibles ou données à caractère hautement personnel ; collecte de données personnelles à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit/contrat.

[70] Article 75, alinéa2, de la LPDCP.

l'accomplissement de ses missions. En outre, il peut saisir l'Instance de protection des données à caractère personnel des difficultés qu'il rencontre dans l'exercice de ses missions[71].

Puisque qu'aucune règle ne peut prétendre être respectée en l'absence de dissuasions, le législateur a donc prévu des sanctions plus ou moins dissuasives devant assurer le respect des dispositions de la nouvelle loi relative à la protection des données à caractère personnel.

B. Les sanctions

Avant de sanctionner tout manquement, l'Instance de protection des données à caractère personnel prononce des injonctions. Il s'agit : d'un avertissement à l'égard du responsable du traitement ne respectant pas ses obligations ; d'une mise en demeure de faire cesser les manquements[72].

Lorsque la mise en demeure s'avère infructueuse, l'Autorité de protection peut prendre des sanctions à l'encontre du contrevenant. Il peut s'agir de sanctions administratives (1) ou pénales (2). Ces sanctions peuvent être infligées sans préjudice d'éventuelles condamnations à verser des dommages-intérêts aux victimes notamment pour traitements frauduleux ou manquements du responsable de traitement à ses obligations.

1. Les sanctions administratives

Sur le plan administratif, l'Instance de protection des données à caractère personnel peut procéder à un retrait provisoire de l'autorisation accordée pour une durée de trois mois. Si au terme de ce délai des mesures correctives n'ont pas été prises, le retrait de l'autorisation devient alors définitif[73]. Il s'agit ici d'une reprise des sanctions prévues dans le cadre de l'Acte additionnel de la CEDEAO[74].

L'IPDCP peut également infliger une amende maximale de cent millions de francs CFA[75]. L'absence de *minima* dans la fixation de l'amende administrative peut poursuivre au moins trois objectifs. Le premier objectif est d'infliger l'amende en fonction du manquement. Le

[71] Article 75, alinéa 1, de la LPDCP.
[72] Article 70 de la LPDCP.
[73] Article 71.1 de la LPDCP.
[74] Voir l'article 20 de l'Acte additionnel.
[75] Article 71.2 de la LPDCP.

deuxième objectif est de permettre à l'Autorité de considérer l'importance des moyens du responsable du traitement : un établissement public togolais et Google n'ont sûrement pas les mêmes moyens financiers, de même une personne physique n'a peut-être pas les mêmes moyens qu'une personne morale. Le troisième objectif serait de pouvoir infliger, assez aisément, la plus lourde sanction pécuniaire aux plus gros portefeuilles en cas de violation de la LPDCP.

Toutefois, on peut se demander si pour de grandes entreprises transnationales, à l'instar de Facebook ou Google, l'amende pécuniaire maximale de cent millions (100.000.000) de francs CFA, environ cent soixante-cinq mille (165.000) dollars, est assez dissuasive pour leur « portefeuille ». En droit européen, à titre comparatif, les violations des dispositions peuvent faire l'objet, d'amendes administratives pouvant s'élever jusqu'à vingt millions (20.000.000) d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[76].

Si, parmi les sanctions administratives, le retrait définitif de l'autorisation donnée par l'Instance de protection des données à caractère personnel semble être celle la plus dissuasive, qu'en est-il des sanctions pénales dont les responsables de traitement peuvent faire l'objet ?

2. Les sanctions pénales

Les actes suivants sont, entre autres, sanctionnées pénalement : le non-respect des formalités préalables ; le non-respect des mesures de retrait provisoire de l'autorisation accordée ; le traitement frauduleux de données personnelles ; le non-respect du droit d'opposition des personnes concernées par le traitement ; la divulgation non autorisée de données personnelles ; l'entrave à l'action de l'IPDCP[77].

La plupart des condamnations pénales varient entre trois mois à cinq ans pour les peines de prisons et pour les amendes entre cent mille et vingt millions de francs CFA. L'amende peut aller jusqu'à vingt-cinq millions (25.000.000) de francs CFA en cas de traitement illicite de données ayant pour fin la recherche dans le domaine de la santé[78], encore en cas de

[76] Voir en ce sens l'article 83.4 et 5 du RGPD.
[77] Article 79 et suivants de la LPDCP.
[78] Article 88 de la LPDCP.

détournement de finalité du traitement[79]. Les peines de prisons et d'amende peuvent être prononcées séparément ou cumulativement.

Si le cumul d'une peine de prison et d'une amende peut s'avérer dissuasive, ce n'est sûrement pas le cas d'une simple amende de vingt-cinq millions (25.000.000) de francs CFA, équivalant à environ trente-huit mille (38.000) euros. La législation française prévoit par exemple une amende de trois cent mille (300.000) euros, cumulée à une peine d'emprisonnement de cinq ans[80].

Par ailleurs, puisque l'Acte additionnel de la CEDEAO relatif à la protection des données à caractère personnel laisse une marge de manœuvre aux États membres dans la détermination des sanctions applicables, il est à craindre un énorme déphasage entre les différentes législations. La différence entre les sanctions pécuniaires prévues par les États-membres est assez ostentatoire. De ce fait, l'absence d'harmonisation permet alors aux structures responsables des traitements des données à caractère personnel de s'établir dans les pays avec une législation moins restrictive.

Somme toute, l'application de la loi relative à la protection des données à caractère personnel est un immense chantier. Pour ce faire, le législateur a prévu des assouplissements. Ainsi, à titre dérogatoire, les traitements de données opérés pour le compte de l'État, d'un établissement public, d'une collectivité locale ou d'une personne morale de droit privé gérant un service public et déjà créés – à la date d'entrée en vigueur de la loi - ne sont soumis qu'à une obligation de déclaration[81]. Quant aux traitements en cours, les responsables de traitement – et leurs sous-traitants – disposent de deux ans pour les traitements de données opérés pour le compte de l'État, d'un établissement public, d'une collectivité territoriale ou une personne morale de droit privé chargée d'une mission de service public[82].

Les autres traitements pour le compte de personnes – ne relevant pas des conditions précitées – ne disposent quant à eux que d'un an à compter de l'entrée en vigueur de la loi pour s'y conformer. Il s'agit principalement dans ce cas des personnes privées. Si cela peut sembler

[79] Article 91 de la LPDCP.
[80] Article 226-16 et suivants du Code pénal français.
[81] Article 94 de la LPDCP.
[82] Article 95.1 de la LPDCP.

facile pour les GAFAMA[83] – déjà dans le bain avec l'entrée en vigueur du RGPD le 25 mai 2018 – on peut s'interroger sur le sort des petites entreprises notamment de e-commerce. Ces dernières peuvent elles se mettre à jour dans ce laps de temps en l'absence de moyens d'accompagnements adéquats ? Outre les personnes privées, avec les récentes élections locales au Togo, le chantier sera aussi colossal pour les collectivités territoriales même si elles disposent de deux ans pour le mener à terme.

La loi togolaise relative à la protection des données à caractère personnel est aussi ambitieuse qu' « utopiste ». Elle est ambitieuse dans la mesure où elle épouse son temps et les défis à relever en matière de protection des données personnelles. Elle reste utopiste en minimisant – du moins à première vue – le temps et l'investissement nécessaires à ce qu'aussi bien les personnes publiques que les personnes privées – État, collectivités territoriales, établissement public, entreprises de e-commerce, etc. – puissent se mettre en conformité. Le rendez-vous est donc pris pour octobre 2020 pour faire un premier bilan, à mi-parcours, de l'application de la LPDCP dans le secteur privé.

Dessa-nin Ewèdew Awesso

[83] Google, Apple, Facebook, Amazon, Microsoft, Alibaba.