



LA PROTECTION DES DONNEES PERSONNELLES RECUEILLIES PAR LE SYSTEME DE GEOLOCALISATION

Pr. Steve SINGAULT NDINGA

digodou@yahoo.fr

DOI: <https://zenodo.org/records/10718995>

RÉSUMÉ

La protection des données personnelles recueillies par le système de géolocalisation est un enjeu crucial dans notre ère numérique. Cette technologie permet de suivre en temps réel les déplacements des individus, mais elle soulève des préoccupations majeures en matière de vie privée et de respect des droits fondamentaux. Objectifs de l'étude ce sont: Analyser les enjeux de la protection des données personnelles dans le contexte de la géolocalisation. Examiner les obligations légales des responsables de traitement en matière de collecte, de traitement et d'exploitation des données géolocalisées. Évaluer les sanctions et recours disponibles en cas de non-respect de ces obligations. Méthodologie utilisée : Revue de la réglementation nationale et internationale sur la protection des données à caractère personnel. Analyse des pratiques des entreprises utilisant des systèmes de géolocalisation. Étude de cas sur les sanctions et les recours appliqués en cas de violation des droits à la vie privée et à la protection des données personnelles. Pour garantir cette protection, tout organisme ou entreprise utilisant un système de géolocalisation doit se conformer à la réglementation en vigueur sur la protection des données à caractère personnel. Cela implique notamment de procéder à une déclaration préalable auprès des autorités compétentes et de respecter des principes stricts en matière de collecte, de traitement et d'exploitation des données. En cas de non-respect de ces obligations légales, les responsables de traitement s'exposent à des sanctions pécuniaires et à des poursuites judiciaires. Les individus dont les données ont été collectées de manière illégale ou

utilisées de manière abusive ont également le droit de demander réparation du préjudice subi. Ainsi, la protection des données personnelles dans le contexte de la géolocalisation nécessite une réglementation stricte et une vigilance continue pour préserver les droits et la vie privée des individus.

INTRODUCTION

Les technologies de l'information et de la communication sont au service de chaque citoyen et ne doivent pas porter atteinte ni aux droits de l'homme ni à la vie privée». Ce grand principe général de droit¹ vient d'être rappelé² pour la première au Gabon, par le gendarme gabonais en charge de la protection des données à caractère personnel³, lors

¹ Voir l'article 3 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, in Journal Officiel de la République Gabonaise n° 74 du 24 au 31 octobre 2011. P. 491.

² Voir la Délibération de la formation plénière n°006/2018 du 20 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Axione Gabon S.A, in Journal Officiel de la République Gabonaise n° 14 du 8 au 15 avril octobre 2019. P. 157.

³ Lire l'ouvrage sous la direction d'Alain Bensoussan, *La protection des personnelles de A à Z*, aux Editions Bruyant Abécédaire 2017: p, 06: *Ce dernier estime qu'il s'agit du traitement des données à caractère personnel automatisé en tout ou partie, ainsi qu'au traitement ou non automatisé des données personnelles continues ou appelées à figurer dans un fichier. Aussi, sont-ils exclus les traitements de données à caractère personnel effectués par une personne physique dans le cadre d'une activité strictement*

d'un litige opposant la société Axione Gabon et monsieur M.J.A. par l'utilisation d'un système de géolocalisation sans notification aux employés. Monsieur M.J.A. a saisi par deux fois, la Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP) d'une plainte contre son employeur la société Axione Gabon S.A, au motif d'avoir été licencié suite aux données personnelles fournies par le dispositif GPS, non notifié aux employés et transmises par la Société Loxea, filiale du groupe CFAO. Qu'au soutien de sa plainte, monsieur M.J.A dénoncé auprès de l'organe de protection le fait qu'Axione Gabon ait utilisé la géolocalisation illégalement et dont le traitement et l'exploitation de ses données à caractère personnel par le moyen d'un GPS sans autorisation, ni consentement préalable et donc, de façon frauduleuse, en violation flagrante de sa liberté, ses droits et intérêt légitime et ayant débouché injustement sur sa mise au chômage prolongé aux conséquences dramatiques.

Le directeur de Concession d'Axione Gabon S.A réfute toute atteinte aux données à caractère personnel de monsieur M.J.A et argue qu'elle n'est pas propriétaire du véhicule litigieux. Elle loue des véhicules auprès de la société Loxea, filiale du groupe CFAO. Or, ces véhicules en location de longue durée sont depuis l'origine pourvus d'un système de GPS pour des raisons évidentes de sécurité. Qu'en outre, non seulement le contrat de location suscité est sur notre base de données et peut être consulté, à tout moment, par tout le personnel surtout les cadres, catégorie à laquelle appartient le plaignant. Mais mieux, ces véhicules sont mis à disposition de l'ensemble des collaborateurs, selon les nécessités de service et qui ne sont pas à usage unique d'un collaborateur, même s'il peut y avoir un usage préférentiel pour un collaborateur dans le cadre des trajets domicile/travail. Qu'en conséquence, le véhicule litigieux ne lui était pas particulièrement et exclusivement affecté, de sorte qu'en aucun cas des données à caractère personnel liées à ce collaborateur n'ont pu être enregistrées par le GPS comme l'illustre un extrait des parcours, lieux et date ci-joints comme pièce à conviction.

A l'examen du dossier soumis à l'appréciation de la CNPDCP, le Gendarme de la protection des données à caractère personnel observe qu'au sens de l'article 3 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel: les technologies de l'information et de la communication doivent être au service de chaque citoyen et qu'elles

personnelle ou domestique. Mais sont également concernés par la protection, les traitements de données qui sont une association de données à caractère personnel du domaine privé et du domaine professionnel.

ne doivent pas porter atteinte, ni à la liberté, ni à l'identité humaine, ni aux droits de l'homme ni à la vie privée, ni aux libertés individuelles ou publiques. Aussi, au terme de l'article 6 tiret 7 de la loi susvisée, on entend par donnée à caractère personnel: 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. Qu'au sens de l'article 51, les traitements automatisés des données à caractère personnel font l'objet d'une déclaration auprès de la Commission Nationale pour la Protection des Données à Caractère Personnel. Que la société Axione Gabon, ne dispose pas d'une autorisation ou d'une déclaration préalable à la mise en œuvre d'un traitement relatif à la géolocalisation auprès de la CNPDCP. Que par ces motifs, **elle** prononce une sanction pécuniaire de 5 millions de franc CFA. Cette décision est susceptible de faire l'objet d'un recours auprès du Conseil d'Etat dans un délai de deux (2) mois à compter de sa notification.

Ainsi, par requête en date du 06 février 2019, la société Axione Gabon S.A saisi le Premier Président du Conseil d'Etat statuant en matière de sursis à exécution, aux fins de sursoir à l'exécution de la délibération n°006/2018 rendue par la Commission Nationale pour la Protection des Données à Caractère Personnel puis de procéder à son annulation. Elle soutient avoir été sanctionnée d'une amende pécuniaire de cinq millions (5.000.000) de francs CFA, en violation flagrante des dispositions des articles 68, 101, et 104 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel. Par ordonnance⁴, le juge des référés estime qu'à la lecture des dispositions de l'article 101 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, la Commission Nationale pour la Protection des Données à Caractère Personnel peut prononcer les mesures suivantes: un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente loi; une mise en demeure de faire cesser les manquements constatés dans le délai qu'elle fixe»; Qu'au regard de l'inobservation par la Commission des mécanismes procéduraux sus rappelés, la délibération incriminée encourt de ce seul fait le sursis à exécution, jusqu'à droit connu sur la

⁴ Voir l'ordonnance affaire Sté Axione Gabon c/ Etat Gabonais (CNPDCP) du 1^{er} avril 2020, répertoire n°07/18-19 rendue par le juge des référés sur ordonnance n°0059/PP-CE/2018-2019 du 19 février 2019 du Premier Président du Conseil d'Etat.

contestation déjà élevée par le demandeur au fond par requête enregistrée au greffe le 06 février 2019.

La Commission va aussitôt former un **recours en rétractation contre l'arrêt du 17 juin 2020. En effet, la Commission va estimer que** cette décision se doit d'être reformée en toutes ses dispositions pour avoir passé outre l'exception d'irrecevabilité tenant au non-respect du recours administratif préalable obligatoire. Aussi, à l'analyse de l'arrêt du 17 juin 2020, la Commission se trouve en droit de conclure que la décision du Conseil d'Etat est entachée d'une interprétation erronée de l'article 108 de la loi n°001/2011 susvisée, en ce qu'il a conféré à la délibération **n°006/2018 du 20 décembre 2018** un caractère juridictionnel, mais également d'une mauvaise interprétation manifeste des dispositions de l'article 101 la loi n°001/2011 susvisée. Dans l'attente de l'issue finale de cette affaire, la question qu'on est en droit de nous poser est celle de savoir si la sanction encourue par la Société Axione Gabon S.A sur le seul fondement d'une atteinte aux données personnelles de monsieur M.J.A est-elle justifiée? En d'autres termes, la Commission était-elle en droit de sanctionner lourdement la société Axione Gabon pour atteinte aux données personnelles de monsieur M.J.A? La réponse à cette interrogation est sans ambiguïté car nonobstant les différentes décisions de justice jusque-là favorables à société Axione Gabon, celle-ci reste un responsable de traitement de fait (I) et mérite la sanction prononcée contre elle par le gendarme de la protection des données à caractère personnel (II).

ÉNONCÉ DU PROBLÈME

Le problème de la protection des données personnelles recueillies par le système de géolocalisation se pose avec acuité dans le contexte du litige opposant la société Axione Gabon et monsieur M.J.A. Ce dernier a été licencié par son employeur, Axione Gabon, suite à des données personnelles fournies par un dispositif GPS installé dans le véhicule mis à sa disposition, données qu'il affirme n'avoir jamais autorisé à être collectées à son insu. Ce litige soulève des questions essentielles concernant le respect de la vie privée et des droits fondamentaux des individus dans un environnement où les technologies de géolocalisation peuvent être utilisées de manière intrusive. La problématique centrale réside dans la légalité et la légitimité de la collecte et de l'utilisation des données personnelles par le biais de la géolocalisation sans notification préalable ni consentement explicite des individus concernés. Cette question se trouve au croisement des impératifs de protection de la vie privée et des droits individuels, d'une part, et des intérêts légitimes des employeurs en matière de gestion des ressources humaines et de

sécurité des biens, d'autre part. Ainsi, le problème majeur soulevé est de déterminer dans quelle mesure les pratiques de collecte et d'utilisation des données personnelles par le système de géolocalisation respectent les normes légales et éthiques en vigueur, tout en assurant un juste équilibre entre les droits des individus et les impératifs opérationnels des entreprises.

OBJECTIFS

- ✓ Évaluer le niveau de conformité des pratiques de collecte et d'utilisation des données personnelles par les systèmes de géolocalisation dans le contexte professionnel, en particulier en ce qui concerne le respect des normes légales et éthiques relatives à la protection de la vie privée et des données personnelles.
- ✓ Identifier les éventuelles lacunes ou failles dans les politiques et les procédures mises en place par les entreprises pour encadrer l'utilisation des technologies de géolocalisation, en mettant en lumière les risques potentiels d'atteinte à la vie privée et aux droits individuels des employés.
- ✓ Proposer des recommandations pratiques et des mesures correctives visant à garantir une utilisation responsable et éthique des systèmes de géolocalisation dans le milieu professionnel, tout en préservant les droits fondamentaux des individus et en assurant la conformité aux réglementations en vigueur en matière de protection des données personnelles.

MÉTHODOLOGIE

La méthodologie de cette étude repose sur une approche mixte combinant à la fois des analyses documentaires et des investigations sur le terrain. Voici les différentes étapes de la méthodologie. Collecte exhaustive de la législation nationale et des réglementations en vigueur concernant la protection des données personnelles, notamment la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel. Revue des décisions judiciaires et administratives pertinentes relative's aux litiges concernant l'utilisation des systèmes de géolocalisation et la protection des données personnelles. Étude des rapports et recommandations émanant d'organismes de régulation et de protection des données personnelles, tels que la Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP). Entretiens semi-directifs avec les parties prenantes impliquées dans les litiges liés à l'utilisation des systèmes de géolocalisation, notamment les employeurs, les employés concernés, les représentants syndicaux et les experts en protection des données.

REU DE LA LITTÉRATURE

La fonction de géolocalisation est activée directement dans les réglages de votre terminal et vous devez donc accepter que le Service puisse y avoir recours. Vous pouvez retirer à tout moment votre consentement en modifiant l'autorisation de la fonction de géolocalisation dans les paramètres de votre terminal comme indiqué ci-dessus. Bien que toute donnée de géolocalisation ne constitue pas une donnée personnelle, les données de géolocalisation collectées par les applications mobiles sont considérées comme telles du moment où elles permettent **de remonter à la personne concernée directement** ou par recoupement avec d'autres informations.

La localisation semble d'ailleurs constituer **l'une des données les plus collectées** sur l'utilisateur. Lors du téléchargement des applications mobiles, il est en effet facile de récupérer cette donnée. Bien que certaines applications disposent de raisons légitimes permettant de justifier cet accès, d'autres procèdent à cette collecte sans que cela ne soit indispensable pour le service proposé. Et même dans le cas où le recueil de ces données est justifié, il doit être limité à des moments bien précis et aux seules données strictement nécessaires. L'intensité et la fréquence d'accès à cette information ont ainsi été remises en cause dans une étude publiée par la CNIL en raison de leur **excessivité**². Les fois où il y a eu accès à ces données sont nombreuses, et il ne s'agissait pas d'applications de navigation ou d'itinéraire. Au vu de la nature de ces données, cette collecte constitue en quelque sorte une atteinte à l'intimité, ce qui n'est pas sans conséquence pour les individus. Des règles strictes à respecter. Le recours à un dispositif de géolocalisation dans les applications mobiles implique que les entreprises mettent en place un certain nombre de mesures afin d'éviter un traitement non autorisé des données :

Informez les personnes concernées de la collecte et du traitement de leurs données personnelles

Cette information doit non seulement contenir toutes les mentions nécessaires au titre du RGPD mais doit également respecter les exigences liées à la forme de l'article 12 dudit texte. En effet, l'utilisateur doit pouvoir accéder à cette information **sans devoir effectuer un effort particulier** et les informations nécessaires doivent être affichées préalablement au recueil des données afin de permettre à la personne concernée de décider en connaissance de cause quant à la communication ou pas de ses données.

Collecter les données strictement nécessaires

En application du principe de minimisation, seules les données personnelles qui sont **strictement nécessaires** au regard des finalités doivent être collectées. Ainsi, lorsque la finalité peut être atteinte sans le recueil des données de géolocalisation, leur collecte n'est pas tolérée.

Conserver les données pendant la durée nécessaire

Les données personnelles, dont les données de géolocalisation, ne peuvent être conservées que pendant **la durée nécessaire à l'atteinte des finalités**. Passé ce délai, les données doivent être supprimées, à moins qu'il ne soit nécessaire de les archiver.

Définir une base légale

Comme pour toutes les données personnelles, il n'est possible de collecter et d'utiliser les données de géolocalisation que si le responsable de traitement a **le droit de le faire**. Ceci exige de respecter l'une des conditions de licéité de l'article 6 du RGPD. De manière générale, la collecte de données de géolocalisation par les applications mobiles nécessite au préalable l'obtention de l'accord de la personne concernée, à moins que les données ne soient anonymisées ou que leur collecte ne soit tolérée pour des finalités liées à la sauvegarde de la sécurité publique et que cette utilisation soit nécessaire, appropriée et proportionnée. Ce consentement doit être **collecté pour chaque finalité** pour répondre au critère de spécificité du consentement. Ainsi, les raisons pour lesquelles ces données sont recueillies doivent être affichées et l'utilisateur doit pouvoir donner son accord pour chacune d'elle. Il doit pouvoir également choisir **le niveau de détail recueillis**, à savoir le pays, la ville, le code postal, etc... Dans ses lignes directrices de 2011, le G29 avait recommandé en plus que l'information sur l'activation de cette fonctionnalité soit **affichée via une icône** tant qu'elle est activée et que cette icône soit visible sur chacun des écrans. Par ailleurs, l'utilisateur doit avoir la possibilité de **revenir sur son choix** à tout moment tout en ayant la possibilité de continuer à utiliser l'application. Il doit en plus pouvoir procéder à la suppression de toute donnée de localisation stockée sur le dispositif de manière définitive.

ANALYSE DES DONNÉES ET DISCUSSION

I/ Un responsable de traitement de fait

La collecte, le traitement ou l'exploitation des données à caractère personnel de manière automatisé ou non et notamment pour tout système de géolocalisation par les organismes privés, doivent faire l'objet d'une déclaration préalable (A) auprès de la Commission Nationale de Protection des Données à caractère

Personnel afin de ne pas porter atteinte aux données personnelles (B)

A/ Un traitement des données à caractère personnel sans déclaration préalable

Le traitement des données à caractère personnel est réglementé en République Gabonaise. Il existe en effet, les formalités préalables à la mise en œuvre des traitements des données à caractère personnels par les personnes publiques (1) tout comme Les formalités préalables à la mise en œuvre des traitements des données à caractère personnels par les personnes privées (2).

1/ Les formalités préalables à la mise en œuvre des traitements des données à caractère personnels par les personnes publiques

Il existe en droit gabonais des formalités préalables pour collecter et traiter les données à caractère personnel au Gabon. Si le Gouvernement, personne publique par excellence veut collecter, exploiter ou traiter des données personnelles, il doit solliciter un avis motivé⁵ de la Commission Nationale de Protection des données à caractère personnel. A cet effet, L'article 55 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel dispose que: «*sont autorisés, par arrêté du ou des Ministres compétent, après avis motivé et publié de la Commission Nationale pour la Protection des Données à Caractère Personnel, les traitements des données à caractère personnel mis en œuvre pour le compte de l'Etat et qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique, ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.*

2/ Les formalités préalables à la mise en œuvre des traitements des données à caractère personnels par les personnes privées

Axione Gabon S.A étant une société privée, elle doit se conformer à la réglementation nationale sur la

⁵La Commission est consultée sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements automatisés. En outre le Gouvernement de la République doit tenir informer la Commission de l'évolution des technologies de l'information. La CNPDCP rend public le cas échant son appréciation des conséquences qui en résultent en matière d'exercice des droits et libertés, puis propose au gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques d'informations (article 34 point 4 et s de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel)

protection des données à caractère personnel. En effet, au terme de l'article 51, alinéa 1 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel dispose que: «*A l'exception de ceux qui relèvent des dispositions prévues aux articles 54, 55 et 56 ou qui sont visés à l'article 65 de la présente loi, les traitements automatisés des données à caractère personnel font l'objet d'une déclaration auprès de la commission nationale pour la protection des données à caractère personnel*». En outre, l'article 52, alinéa 3 de la loi susvisée dispose que: «*la Commission délivre sans délai un récépissé, le cas échéant, par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de ce récépissé; il n'est exonéré d'aucunes de ses responsabilités*». A cet effet, le récépissé de déclaration est accompagné par une norme simplifiée⁶ qui encadre les données fournies par GPS. La société Axione Gabon n'avait pas suivie cette procédure et n'était pas détentricrice de la norme simplifiée. Par ailleurs, l'organisme privé doit satisfaire aux conditions énoncées à l'article 58 de la loi susvisée, ainsi qu'il suit : justifier la **dénomination et la finalité du traitement**. Au sens de la loi n°001/2011 susvisée, les données à caractère personnel ne peuvent être collectées que pour des finalités déterminées, explicites, légitimes non inhumaines et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités⁷. Or, le constat amer qui se dégage est que, la Société Axione Gabon a opéré un détournement de finalité.

B/ Une atteinte aux données à caractère personnel du sieur M.J.A

Pour porter atteinte aux données personnelles de M.J.A, il fallait au préalable montrer que les données issues du système GPS sont bien des données à caractère personnel (1) et que la société Axione n'a fait qu'exploiter sans être officiellement un sous-traitant (2)

⁶ Voir la Délibération n°016/CNPDCP du 23 mai 2019 portant norme simplifiée n°003 relative à l'exploitation de la géolocalisation des véhicules.

⁷ La Délibération n°016/CNPDCP du 23 mai 2019 portant norme simplifiée n°003 relative à l'exploitation de la géolocalisation des véhicules tout comme la Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public NOR

1/ Les données issues d'un système de géolocalisation⁸ sont des données à caractère personnel

La géolocalisation est une technique qui permet de prendre connaissance à un instant donné ou en continu, la vitesse, la date et heure de circulation, le trajet effectué et partant, la surveillance des déplacements dans le temps et dans l'espace des conducteurs des véhicules pourvus de GPS.

Ce système a été utilisé par la société Axione Gabon pour suivre les mouvements dans l'espace et dans le temps de monsieur M.J.A. Le dispositif de géolocalisation va consister à recueillir des données personnelles rattachées à **monsieur M.J.A.** Dans le procès-verbal de l'entretien préalable au licenciement tenu le 15 février 2018, Axione Gabon a exposé les raisons de la tenue de l'entretien, en rappelant au sieur M.J.A les faits qui lui sont reprochés par la Direction et notamment de nombreux retards non justifiés⁹. L'employeur va présenter au sieur M.J.A le relevé des entrées et sorties de la station ainsi que les relevé GPS du véhicule de service de ce dernier prouvant l'utilisation du véhicule les jours mentionnés. Pourtant rétorque le sieur M.J.A, il n'avait pas l'obligation d'aller au travail signer une feuille de présence avant de partir directement en rendez-vous clientèle.

2/ La non reconnaissance de la qualité officielle de sous-traitant des données à caractère personnel recueillies par géolocalisation¹⁰

Au terme de la délibération n°005/2018 du 03 octobre 2018 portant avis relatif à la plainte de monsieur M.J.A contre la société Axione, c'est la société Loxea, filiale

⁸ Les données à caractère personnel correspondent à toutes les données permettant d'identifier une personne ou de la rendre identifiable raisonnablement. Cette identification peut résulter directement ou indirectement de caractéristiques telles que: le nom, la photo, l'empreinte digitale ou biométrique, identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

⁹ Jeudi 1^{er} juin 2017 à 10h21; 8 juin à 10h 17; 5 juillet à 14h46; 19 juillet à 9h56 pourtant véhicule parti du domicile à 9h36; 31 juillet à 11h41 véhicule parti du domicile à 5h26; 22 août 2017 à 11H05 véhicule parti du domicile à 10H40. Par ailleurs l'employeur dénonce une utilisation anormale et intense du véhicule de service à des fins non justifiées et parfois à des heures tardives.

¹⁰ Dans un arrêt de la CJUE, aff c-131/12 du 13/05/2014, le haut juge Communautaire européen estime que: En tenant compte des innovations technologiques telles que l'internet des objets et la géolocalisation, sont désormais considérés comme des données à caractère personnel, à savoir

du groupe CFAO, qui loue les véhicules dotés de système géolocalisation à la société Axione Gabon SA et inexplicablement, lui transmet également des données collectées issues dudit système pour exploitation. Pouvait-on dès lors considérer Axione Gabon comme sous-traitant des données personnelles collectées par Loxea, qui serait vu ici, comme un responsable de traitement?. La sous-traitance est une opération par laquelle une entreprise (le donneur d'ordre) confie à une autre entreprise (le sous-traitant) le soin d'exécuter pour elle une partie des actes de production et de service dont elle conserve la responsabilité. C'est le même principe en matière de traitement des données personnelles. La sous-traitance est un phénomène économique très développé en matière numérique car le traitement des données personnelles se prête tout particulièrement à l'externalisation du stockage des données. Il s'agit pour un responsable de traitement de confier le traitement ou l'exploitation de données en totalité ou en partie à une autre entreprise prestataire, le sous-traitant. Toutefois, en cas de recours aux services d'un sous-traitant, ce dernier ne peut agir que sur instruction du responsable du traitement, lequel n'est pas dispensé de son obligation de veiller au respect des mesures de sécurité qui lui sont imposées par l'article 66 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel.

II/ L'engagement de la responsabilité d'Axione Gabon

N'ayant pas respecté la législation gabonaise en matière de protection des données à caractère personnel et de s'être immiscé dans la vie privée de son salarié, la société Axione Gabon, ne pouvait que voir sa responsabilité engagée sur le fondement d'une atteinte à la vie privée (A) et se voir appliquée souverainement une sanction pécuniaire (B)

A/Une responsabilité pour atteinte à la vie privée¹¹ du sieur M.J.A

Pour retenir la responsabilité de la société Axione Gabon, le gendarme de la protection des données personnelle retient fort justement, une intrusion dans la vie privée de M.J.A (1) puis, une méconnaissance des droits fondamentaux de ce dernier par rapport à ses données personnelles (2)

¹¹ Lire l'ouvrage de Fabrice Mattatia, *RGPD et Droit des données personnelles*, 5^e édition Eyrolles, 2021. P.8. Celui-ci dit que la vie privée est un concept récent d'un point de vue aussi bien sociologique et juridique. Qu'Aristote a distingué la vie publique du citoyen et la vie familiale, alors que pour Montaigne, on est libre que si l'on peut s'isoler pour réfléchir dans la sphère privée.

1/ Une intrusion dans la vie privée du sieur M.J.A

La notion de vie privée est fluctuante et imprécise. Elle est dépendante des circonstances et entendue largement par les autorités de protection des données et au final par les tribunaux, afin d'assurer une protection plus forte. L'intimité des relations personnelles constitue le cadre classique de la vie privée. Et même là, il reste que même dans sa dimension personnelle, la notion de la vie privée a toujours été entendue largement et ne s'est jamais prêtée à une définition exhaustive. La Cour Européenne des Droits de l'Homme a déclaré recevable dans une affaire, une requête fondée sur le refus d'écarter des débats des lettres privées à caractère amoureux devant le juge du divorce¹²

En principe, dès que l'exploitation d'un service de géolocalisation implique la collecte et le traitement des données à caractère personnel, le service est soumis à la réglementation sur la protection de la vie privée. Cette technologie rend possible la surveillance des déplacements d'un individu dans le temps et dans l'espace et peut donner lieu à certaines dérives puis nuire à la vie privée, d'où la nécessité de son encadrement par la loi. Aussi, peuvent être considérés comme relevant de la vie privée ou de l'intimité d'un individu, la vie sentimentale, les relations amicales, la nudité, les pratiques sexuelles, l'état de santé, les moyens d'existence, les convictions religieuses, politiques ou syndicales. Par contre la vie privée dans les projets numériques prend en compte d'autres considérations¹³.

La technique de géolocalisation constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit encadrée¹⁴ par la loi et exécutée sous contrôle d'un juge¹⁵. En effet, la

¹² Voir Dc, CEDH du 9 février 2006, NN et TA c/Belgique, NO 65097, 2001.

¹³ Lire le rapport sur la question publiée en 2016 de messieurs Alessandro Zamboni, Jérôme Billois, Raphael Brun et Youri Dufau Sansot, *La vie privée à l'ère du numérique: au delà de la conformité, un enjeu de confiance*, in WWW.WAVESTONE.Com. P. 9

¹⁴ Selon Jean François Renucci, *Traité de Droit Européen des droits de l'Homme*, Edition LGDJ, 2007.p.233, « Il s'agit de protéger l'individu non seulement contre l'ingérence des pouvoirs publics mais aussi contre celle des particuliers et des institutions privées y compris les moyens de communications de masse » Mieux, la mémorisation des données personnelles par une autorité publique ou privée est une ingérence dans le droit au respect de la vie privée. Une telle pratique n'est donc admissible que si les conditions d'ingérence sont remplies, notamment l'exigence de garantie adéquate.

¹⁵ Voir le magazine en ligne Lgalis : l'actualité du droit des nouvelles technologies

géolocalisation permet aujourd'hui d'obtenir avec une certaine précision qui pourrait être de l'ordre de 10 mètres la position géographique d'un véhicule et de suivre ses éventuels déplacements en l'équipant d'un récepteur GPS doté d'un système GPRS qui transmet cette position par un réseau de téléphonie mobile¹⁶. Il s'agit d'un dispositif permettant de localiser, à tout moment et en temps réel un individu ou un objet, soit par l'utilisation d'un dispositif dédié tel qu'une balise, soit par le suivi dynamique d'un terminal de communication. En fait, la géolocalisation en temps réel constitue une technique spéciale qui permet de suivre en direct le déplacement d'une personne. Il existe deux méthodes pour y procéder. D'une part, le suivi dynamique d'un terminal de télécommunication avec l'exploitation de la technologie propre d'un téléphone, d'une tablette ou d'un véhicule équipé d'un système GPS. D'autre part, un dispositif matériel directement installé sur un moyen de transport ou un autre objet, à l'instar d'une balise. Ces moyens en règle générale sont susceptibles de porter atteinte au droit d'une personne, au respect de sa vie privée en ce qu'elles révèlent plus d'information sur sa conduite les opinions ou les sentiments de la personne qui en fait l'objet¹⁷.

2/ Une méconnaissance des droits fondamentaux d'un salarié par rapport à ses données personnelles.

Monsieur M.J.A à plusieurs droits reconnus par la loi au regard des données le concernant dont la société Axione Gabon avait aussi l'obligation de préciser les modalités d'exercice de ces droits L'article 9 de la Charte africaine des droits de l'homme et des peuples du 26 juin 1981, alinéa 1 et 2, dispose que toute personne a droit à l'information et toute personne a le droit d'exprimer et de diffuser ses opinions dans le cadre des Lois et règlements. L'information préalable des employés quant à l'utilisation des véhicules équipés de système de géolocalisation par Axione Gabon S.A n'a pas été respectée conformément à la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel. En effet, toute personne a le droit d'interroger le responsable d'un fichier pour savoir s'il détient des informations sur elle et le cas échéant d'en obtenir la communication.

2941 Décisions en ligne, Jurisprudence : Vie privée du mercredi 06 novembre 2013 : Cour de cassation Chambre criminelle Arrêt du 22 octobre 2013 Mohamed X. / Ministère public.

¹⁶ Lire Martini Matsopoulou, *La surveillance par géolocalisation à l'épreuve de la convention européenne des droits de l'homme*, in Recueil Dalloz, 2011. P. 724.

¹⁷ C'est la substance de l'arrêt de la CEDH 2010 UZUN c/ Allemagne affaire n35623/05 §52. Extrait.

Ce droit fondamental d'accès à ses propres informations n'a pas pu être exercé par M.J.A. Dans le cas de M.J.A, le fichier n'était pas accessible parce que inconnu des salariés. Alors que conformément aux dispositions de l'article 59 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, les employés d'Axione Gabon concernés par les véhicules de service, devraient être informés, préalablement à l'exploitation de leurs données personnelles recueillies par GPS de : l'identité du propriétaire des véhicules de service pourvus de GPS; la finalité¹⁸ poursuivie par l'exploitation issue des données recueillies par GPS, les destinataires ou catégories des destinataires des données fournies par GPS.

B/ une sanction pécuniaire justifiée

Pour n'avoir pas respecté les obligations légales d'un responsable de traitement en s'immiscant dans la vie privée de monsieur M.J.A, la société Axione Gabon SA s'est exposée à une sanction pécuniaire adaptée à la gravité du manquement (2) appréciée souverainement (1) par le gendarme de la protection des données personnelles.

1/ L'appréciation souveraine du type de sanction

Lorsqu'il s'agit de protéger les droits individuels des citoyens contre l'utilisation abusive de l'informatique par la puissance publique mais aussi par les personnes privées, certaines autorités administratives vont se voir doter d'un pouvoir réglementaire ou plus généralement d'un pouvoir de sanction¹⁹. En effet, il existe des entités administratives qui ne sont pas soumises au pouvoir hiérarchique et ne peuvent non plus être soumises à la tutelle administrative, constituant ainsi des autorités administratives indépendantes (AAI), c'est le cas de la CNPDCP qui a reçu du législateur une mission de protection des données à caractère personnel.

Etant donné que la Commission a été saisie d'une plainte pour violation des données personnelles par un responsable de traitement de fait, la Commission avait à bon droit prononcé à l'encontre de ladite société, une sanction pécuniaire d'un montant de cinq

¹⁸ Selon l'ouvrage de Céline Castels Renard, *Quelle protection des données personnelles en Europe*, Edition Larcier, 2015. P.19, la finalité d'une collecte ou d'un traitement est double: elle permet dans un premier temps de justifier et rendre licite et dans un second temps, de fonder une sélection des données collectées nécessaires pour remplir la finalité déterminée.

¹⁹ Lire l'ouvrage d'André Legrand et de Céline Wiener, *Droit public*; La Documentation française, Edition 2014, p. 73.

(5) millions de FCFA, en application de l'article 105 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel. Cette sanction pécuniaire prononcée par la CNPDCP ne pouvait par ailleurs pas être regardée comme ayant un caractère juridictionnel comme l'avait soutenu le Conseil d'Etat. La Commission Nationale de Protection des Données à caractère personnel (CNPDCP)²⁰ est une Autorité Administrative Indépendance (AAI), elle est dotée de la personnalité juridique et jouit de l'autonomie administrative et financière²¹.

Le Conseil d'Etat n'est donc pas compétent pour se prononcer sur des actes juridictionnels. Il se serait donc déclaré incompétent pour juger au fond l'affaire Axione Gabon contre la CNPDCP. Le fait d'avoir jugé recevable cette affaire, montre à suffisance que la décision de la CNPDCP n'est qu'un acte administratif et non pas un acte juridictionnel. Dans une célèbre décision²², la Cour Constitutionnelle Gabonaise rappelle le caractère de simple organe administratif les Autorité Administrative Indépendante et qu'une administration publique ne peut rendre des actes juridictionnels. En effet, si le législateur octroie à la Commission des pouvoirs juridictionnels, ce qui serait contraire à la Constitution Gabonaise dont l'article 67 énonce que: « *La justice est rendue au nom du peuple par la Cour Constitutionnelle, les juridictions de l'ordre judiciaire, de l'ordre administratif, de l'ordre financier, de la Haute cour de justice, la Cour de justice de la République et les autres juridictions d'exception* ».

2/Une sanction adaptée à la gravité du manquement observé

Nous avons déjà rappelé qu'au sens de l'article 3 de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel: les technologies de l'information et de la communication doivent être au service de chaque citoyen et qu'elles ne doivent pas porter atteinte, ***ni à la liberté, ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*** Monsieur M.J.A a vu sa vie privée subir

²⁰Créée par la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, agit au nom de l'Etat sans pour autant relever d'un membre du gouvernement.

²¹ Voir l'article 15 de la Loi n°001/2011 relative à la protection des données à caractère personnel.

²² Décision n°11/CC du 10 février 2003 relative à la requête par Monsieur Jean Christophe Nze-Biteghe tendant à voir déclarer inconstitutionnelles certaines dispositions de la loi n°5/2002 portant création, organisation et fonctionnement de la Commission Nationale de la Lutte contre l'enrichissement illicite.

une intrusion grotesque de la part de son employeur en violation flagrante de la loi susvisée. Dans ce cas, le gendarme de la protection des données dispose de divers moyens par lesquels, il peut utiliser pour obtenir le respect de la loi: l'exercice des poursuites pénales, le prononcé de sanctions administratives ou pécuniaires, le recours à l'exécution forcée. En matière de sanction administrative, l'article 101 de la loi susvisée prévoit: l'avertissement et la mise en demeure. L'article 102 prévoit, le retrait provisoire pour une durée de trois mois du récépissé de déclaration ou de l'autorisation d'un traitement de données, le retrait définitif et enfin, une amende pécuniaire d'un million à cent millions de francs CFA.

La mise en place d'un tel système de géolocalisation, ainsi que l'utilisation de ces données nécessitent une autorisation de la Commission Nationale pour la Protection des Données à Caractère Personnel. L'atteinte flagrante de la vie privée et de la liberté individuelle de Monsieur M.J.A constitue un manquement important²³. Le licenciement suite aux données personnelles recueillies illégalement constitue le facteur aggravant qui aurait permis à la Commission et de manière souveraine de faire application de l'article 105, en infligeant une sanction pécuniaire de cinq (5) millions de Francs CFA à l'endroit d'Axione Gabon S.A. Cette sanction pécuniaire n'a jamais été acceptée par la Société Axione Gabon. Celle-ci a toujours affirmé et soutenu en cela par le Conseil d'Etat, que cette décision a été prise en violation de l'article 101 de la loi susvisée, pour n'avoir pas été précédé des préalables obligatoires d'avertissement et de mise en demeure. Cette lecture de la loi ne pouvait prospérer, étant donné qu'Axione Gabon n'a respecté aucune formalité légale et notamment n'était détentrice d'aucun récépissé de déclaration et opérait des traitements de données personnelles en toute illégalité. Ensuite, l'avertissement en réalité n'a qu'un caractère préventif²⁴. Il est

²³ Dans sa dimension personnelle, le droit au respect de la vie privée répond à une approche traditionnelle qu'entend assurer une protection efficace, qu'il s'agisse de la sphère intime des relations personnelles, des données personnelles ou encore des techniques de surveillance des individus, aussi, l'intimité personnelle reste-t-elle le cadre classique de la protection de la vie privée, pour Jean Francois Rennuci, Droit Européen des droits de l'Homme, 8e édition, LGDJ, P.268/

²⁴ Dans une célèbre décision du haut juge judiciaire français: Décision n° 2018-765 DC du 12 juin 2018 sur la loi française relative à la protection des données personnelles, et parlant des décisions arrêtées par le gendarme français de la protection des données à caractère personnel, il est notamment dit que: « *Après avoir rappelé sa formulation de principe en matière de proportionnalité des peines (paragr. 35), le Conseil constitutionnel s'est fondé sur le caractère préventif de l'avertissement, prononcé en amont*

prononcé en réalité à l'endroit d'un responsable de traitement lorsque les opérations de traitements de données personnelles qu'il envisage d'effectuer sont susceptibles de violer les dispositions de la loi n°001/2011 susvisée.

En somme, l'affaire Axione Gabon, toujours pendante devant le Conseil d'Etat Gabonais, tombe à point nommé pour rappeler que la protection des données personnelles est finalement consubstantielle à l'être humain. Cette protection des données s'impose en réaction aux risques²⁵ croissants que la puissance de l'informatique ou des nouvelles technologies font courir aux droits fondamentaux des personnes concernées et dans nos vies. L'encadrement des données personnelles à travers la géolocalisation doit avoir pour objectif d'établir un équilibre entre les droits des personnes et le légitime besoin de collecte, de traitement et d'exploitation de certaines données à caractère personnel sur le plan professionnel.

CONCLUSION

La protection des données personnelles dans le contexte de la géolocalisation est un impératif éthique et juridique dans notre société numérique. L'évolution rapide des technologies de suivi des déplacements nécessite une réglementation stricte pour garantir le respect des droits fondamentaux des individus, notamment le droit à la vie privée. Cette étude a souligné l'importance de la conformité aux obligations légales en matière de collecte, de traitement et d'exploitation des données géolocalisées. Les responsables de traitement doivent se conformer aux exigences de déclaration préalable et respecter les principes de finalité, de légitimité et de sécurité des données. En cas de non-respect de ces obligations, des sanctions pécuniaires et des poursuites judiciaires peuvent être engagées. De plus, les individus concernés ont le droit de demander réparation du préjudice subi en cas d'utilisation abusive de leurs données personnelles. Il est donc impératif pour les entreprises et organismes utilisant des systèmes de géolocalisation de prendre les mesures nécessaires pour garantir la protection des données personnelles et respecter les droits des individus. Cela passe par une sensibilisation accrue, une formation du personnel et

de la commission de tout manquement, pour exclure une qualification punitive

²⁵ L'article premier paragraphe 6 de la Constitution gabonaise met en garde contre les limites de l'usage de l'informatique pour sauvegarder l'Homme, l'intimité personnelle et familiale des personnes, et le plein exercice de leurs droits.

une mise en conformité rigoureuse avec la réglementation en vigueur.

RECOMMANDATIONS

Les entreprises devraient adopter une approche de minimisation des données en ne collectant que les informations strictement nécessaires pour atteindre les objectifs spécifiques du système de géolocalisation. Limiter la collecte de données contribue à réduire les risques liés à la protection de la vie privée et à garantir une utilisation plus éthique des données personnelles. Il est essentiel d'investir dans des mesures de sécurité robustes pour protéger les données personnelles recueillies par les systèmes de géolocalisation contre les cyberattaques et les violations de sécurité. Cela comprend la cryptage des données, l'utilisation de pare-feu et de logiciels antivirus, ainsi que la mise en œuvre de protocoles d'authentification sécurisés. Avant de mettre en œuvre un système de géolocalisation, les entreprises devraient réaliser une évaluation approfondie de l'impact sur la vie privée afin d'identifier les risques potentiels pour la vie privée des individus. Cette évaluation devrait prendre en compte les droits des individus, les mesures de sécurité mises en place et les implications éthiques de l'utilisation des données. Les entreprises devraient adopter une approche transparente et responsable dans la gestion des données personnelles. Cela inclut la communication claire des pratiques de collecte et de traitement des données, ainsi que la mise en place de mécanismes de responsabilité interne pour garantir le respect des normes de protection des données et la prise en compte des préoccupations des individus.

RÉFÉRENCES

- [1] C'est la substance de l'arrêt de la CEDH 2010 UZUN c/ Allemagne affaire n35623/05 §52. Extrait.
- [2] Créée par la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, agit au nom de l'Etat sans pour autant relever d'un membre du gouvernement.
- [3] Dans un arrêt de la CJUE, aff c-131/12 du 13/05/2014, le haut juge Communautaire européen estime que: En tenant compte des innovations technologiques telles que l'internet des objets et la géolocalisation, sont désormais considérés comme des données à caractère personnel, à savoir.

- [4] Décision n°11/CC du 10 février 2003 relative à la requête par Monsieur Jean Christophe Nze-Biteghe tendant à voir déclarer inconstitutionnelles certaines dispositions de la loi n°5/2002 portant création, organisation et fonctionnement de la Commission Nationale de la Lutte contre l'enrichissement illicite.
- [5] Décisions en ligne, Jurisprudence : Vie privée du mercredi 06 novembre 2013 : Cour de cassation Chambre criminelle Arrêt du 22 octobre 2013 Mohamed X. / Ministère public.
- [6] Jeudi 1er juin 2017 à 10h21; 8 juin à 10h 17; 5 juillet à 14h46; 19 juillet à 9h56 pourtant véhicule parti du domicile à 9h36; 31 juillet à 11h41 véhicule parti du domicile à 5h26; 22 août 2017 à 11H05 véhicule parti du domicile à 10H40. Par ailleurs l'employeur dénonce une utilisation anormale et intense du véhicule de service à des fins non justifiées et parfois à des heures tardives.
- [7] La Commission est consultée sur tout projet de loi ou décret relatif à la protection des personnes à l'égard des traitements automatisés. En outre le Gouvernement de la République doit tenir informer la Commission de l'évolution des technologies de l'information. La CNPDCP rend public le cas échant son appréciation des conséquences qui en résultent en matière d'exercice des droits et libertés, puis propose au gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques d'informations (article 34 point 4 et s de la loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel)
- [8] La Délibération n°016/CNPDCP du 23 mai 2019 portant norme simplifiée n°003 relative à l'exploitation de la géolocalisation des véhicules tout comme la Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les

employés d'un organisme privé ou public
NOR

[9] Les données à caractère personnel correspondent à toutes les données permettant d'identifier une personne ou de la rendre identifiable raisonnablement. Cette identification peut résulter directement ou indirectement de caractéristiques telles que: le nom, la photo, l'empreinte digital ou biométrique, identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

[10] Lire l'ouvrage d'André Legrand et de Céline Wiener, Droit public; La Documentation française, Edition 2014, p. 73.

[11] Lire l'ouvrage de Fabrice Mattatia, RGPD et Droit des données personnelles, 5e édition Eyrolles, 2021. P.8. Celui-ci dit que la vie privée est un concept récent d'un point de vue aussi bien sociologique et juridique. Qu'Aristote a distingué la vie publique du citoyen et la vie familiale, alors que pour Montaigne, on est libre que si l'on peut s'isoler pour réfléchir dans la sphère privée.

[12] Lire le rapport sur la question publiée en 2016 de messieurs Alessandro Zamboni, Jérôme Billois, Raphael Brun et Youri Dufau Sansot, La vie privée à l'ère du numérique: au delà de la conformité, un enjeu de confiance, in WWW.WAVESTONE.Com. P. 9

[13] Lire Martini Matsopoulou, La surveillance par géolocalisation à l'épreuve de la convention européenne des droits de l'homme, in Recueil Dalloz, 2011. P. 724.

[14] Selon Jean François Renucci, Traité de Droit Européen des droits de l'Homme, Edition LGD, 2007.p.233, « Il s'agit de protéger l'individu non seulement contre l'ingérence des pouvoirs publics mais aussi contre celle des particuliers et des institutions privées y compris les moyens de communications de masse » Mieux, la mémorisation des données personnelles par une autorité publique ou privée est une ingérence dans le droit au respect de la vie privée. Une telle pratique n'est donc admissible que si les conditions d'ingérence

sont remplies, notamment l'exigence de garantie adéquate.

[15] Selon l'ouvrage de Céline Castels Renard, Quelle protection des données personnelles en Europe, Edition Larcier, 2015. P.19, la finalité d'une collecte ou d'un traitement est double: elle permet dans un premier temps de justifier et rendre licite et dans un second temps, de fonder une sélection des données collectées nécessaires pour remplir la finalité déterminée.

[16] Voir Dc, CEDH du 9 février 2006, NN et TA c/Belgique, NO 65097, 2001.

[17] Voir l'article 15 de la Loi n°001/2011 relative à la protection des données à caractère personnel.

[18] Voir la Délibération n°016/CNPDCP du 23 mai 2019 portant norme simplifiée n°003 relative à

[19] Voir le magazine en ligne Lgalis : l'actualité du droit des nouvelles technologies