

RÉPONDRE EFFICACEMENT AUX DEMANDES D'EXERCICE DES DROITS : OBLIGATIONS ET BONNES PRATIQUES AU SÉNÉGAL

Rapport sur le webinaire organisé à l'occasion de la Journée internationale de la protection des données (28 janvier 2026)



I. INTRODUCTION

Le 28 janvier 2026, à l'occasion de la Journée internationale de la protection des données, Africa Data Protection (ADP) a organisé un webinaire d'envergure intitulé « Répondre efficacement aux demandes d'exercice des droits : obligations et bonnes pratiques au Sénégal ». Ce webinaire organisé en collaboration avec la Commission de protection des données du Sénégal (CDP) et l'Association africaine des Droits Numériques (ADN) s'inscrivait dans un contexte marqué par une prise de conscience croissante de l'importance de la protection des données personnelles, tant au niveau national qu'international. Le Sénégal dispose d'un cadre juridique solide (notamment la Loi n° 2008-12 portant sur la protection des données à caractère personnel du 25 janvier 2008, ci-après la « Loi 2008-12 »), mais sa mise en œuvre effective reste un défi pour de nombreuses organisations, qu'elles soient publiques ou privées.

L'objectif principal de ce webinaire était de sensibiliser les acteurs (responsables de la protection des données, juristes, représentants d'entreprises, etc.) à leurs obligations légales et de leur fournir des outils concrets pour répondre aux demandes d'exercice des droits des individus. Ces demandes peuvent concerner l'accès aux données, leur rectification, leur suppression ou encore l'opposition à leur traitement. Le webinaire a également visé à renforcer la culture de la conformité et à promouvoir une approche proactive en matière de protection des données.

Dans son introduction, M. Ousmane Thiongane, Président de la CDP, a rappelé que cette loi impose aux organisations de mettre en place des mécanismes clairs et accessibles pour permettre aux individus d'exercer leurs droits. Il a insisté sur le fait que la conformité ne se limite pas à une obligation légale, mais constitue également un gage de confiance pour les citoyens et les clients. Pour les responsables de traitement, les demandes ne doivent pas être perçues comme une contrainte administrative mais comme une opportunité d'améliorer leur pratique, de renforcer leur conformité, et de placer l'utilisateur au cœur des processus de traitement des données personnelles. Cela suppose des procédures claires, des délais maîtrisés, une traçabilité, des réponses et une sensibilisation continue des opérationnels.

A l'occasion de la rentrée solennelle des cours et tribunaux du 22 janvier 2026, le premier président de la Cour suprême a salué le rôle avant-gardiste de la Commission de protection des données à caractère personnel à côté des autres juridictions pour la meilleure protection de la vie privée mais nous rappelle aussi que la protection des données à caractère personnel ne peut rester théorique : elle doit se traduire par des réponses concrètes, diligentes et conformes à la loi. Le rôle de l'autorité de protection des données à caractère personnel est d'encadrer, d'orienter et d'accompagner afin que le respect des droits devienne un réflexe et non une exception.

1.1 LES DROITS DES PERSONNES CONCERNÉES



La Loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel prévoit différents droits pour les personnes concernées, les personnes physiques dont les données à caractère personnel sont traitées par le responsable de traitement : droit d'accès, droit de rectification, droit d'information, droit d'opposition et droit à la suppression de ses données. Ces droits existent, pour la plupart, dans d'autres pays africains, mais aussi au sein de l'Union européenne. Toutefois, lorsqu'on effectue une comparaison rapide, on constate que certains droits prévus par le 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, dit Règlement général sur la protection des données (RGPD) ne figurent pas dans ce cadre juridique, notamment le droit à la portabilité des données à caractère personnel ainsi que l'ensemble des garanties liées à la prise de décision automatisée.

La Loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel prévoit différents droits pour les personnes concernées, les personnes physiques dont les données à caractère personnel sont traitées par le responsable de traitement : droit d'accès, droit de rectification, droit d'information, droit d'opposition et droit à la suppression de ses données. Ces droits existent, pour la plupart, dans d'autres pays africains, mais aussi au sein de l'Union européenne. Toutefois, lorsqu'on effectue une comparaison rapide, on constate que certains droits prévus par le 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, dit Règlement général sur la protection des données (RGPD) ne figurent pas dans ce cadre juridique, notamment le droit à la portabilité des données à caractère personnel ainsi que l'ensemble des garanties liées à la prise de décision automatisée.

1.2 LE RÔLE DE LA COMMISSION DE PROTECTION DES DONNÉES PERSONNELLES DU SÉNÉGAL

La mission de la CDP, qui est une Autorité Administrative Indépendante (AAI), est de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la Loi 2008-12 notamment les principes directeurs pour la mise en œuvre des traitements de données à caractère personnel qui sont : la finalité, la licéité, le recueil de consentement, la sécurité, la confidentialité et la conservation des données. La CDP veille à ce que les traitements de données à caractère personnel ne portent pas atteinte à la vie privée, notamment par le biais de contrôles a priori et a posteriori.

Madame Marième Sangaré, Directrice des Affaires Juridiques, de la Conformité et du Contentieux de la CDP, rappelle que la CDP est la gardienne de la vie privée des citoyens sénégalais; elle se doit donc de bien contrôler les données qui font l'objet de traitement au niveau des responsables de traitement. L'exercice des droits est un point très sensible qui est pris en compte aussi bien en amont (à travers les formalités préalables) qu'en aval. En pratique, la CDP s'assure que les responsables de traitement formalisent la procédure d'exercice des droits des personnes : identifier une personne dédiée au traitement des demandes d'exercice des droits, former cette personne, et tenir à jour un registre des demandes pour pouvoir cartographier les demandes. Au niveau de la session plénière des commissaires, qui est l'organe délibérant, il est arrivé que les commissaires ne délibèrent pas sur les dossiers parce que l'exercice des droits n'est pas très clair, ils disent qu'ils refusent de donner un avis favorable ou défavorable avant que le responsable de traitement ne complète son dossier et envoie

les justificatifs.

Par ailleurs, la CDP joue un rôle déterminant en matière d'accompagnement et de médiation. De nombreux litiges trouvent ainsi une issue grâce à son intervention. Un exemple marquant concerne l'installation de systèmes de vidéosurveillance embarquée dans les camions transportant des hydrocarbures. Cette initiative a suscité une vive polémique : pour les chauffeurs, la cabine constitue un véritable espace de travail et, à ce titre, l'installation de caméras soulève des enjeux sensibles liés au respect de la vie privée et de la dignité humaine. Dans ce contexte, la CDP est intervenue de manière décisive. Elle n'a pas seulement agi en tant qu'autorité de protection des données, mais également comme médiatrice entre les différentes parties prenantes. Ce type de situation exige une approche profondément humaine, qui doit rester au cœur du processus décisionnel. Ainsi, au-delà de son statut d'autorité administrative indépendante, la CDP exerce des missions essentielles de médiation, de sensibilisation et d'accompagnement. Son objectif demeure constant : agir au mieux des intérêts de la population et garantir un équilibre entre innovation, sécurité et respect des droits fondamentaux.



1.3 RETOUR D'EXPÉRIENCE D'UN DPO AU SÉNÉGAL

Monsieur Adama Diouf, DPO du Groupe SONATEL, rappelle le manque de sensibilisation des personnes concernées sur leurs droits et recommande aux responsables de traitement de :

- Prévoir un canal de contact dans les mentions d'information et une adresse email générique pour pouvoir permettre aux personnes concernées d'exercer leurs droits.
- Créer une politique interne de gestion de ces demandes d'exercice de droit qui permet de gérer en interne : procédures de réception, de réponse, de qualification de la demande (demande d'accès, de rectification ou autre) et vérification de la disponibilité des données (s'assurer qu'elles n'ont pas été supprimées pour respecter l'obligation de limitation de durée de conservation) etc.



II. LE CADRE LÉGAL DES DIFFÉRENTES TYPOLOGIES DES DEMANDES D'EXERCICE DES DROITS AU SÉNÉGAL

Les personnes dont les données sont traitées disposent de droits qu'elles peuvent exercer auprès de tout organisme qui traite leurs données à caractère personnel. Dans le préambule de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), il est clairement marqué que son ambition est de garantir, « en proposant un type d'ancrage institutionnel, que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques ».

Ces droits ne sont certes pas absolus et doivent être mis en balance avec les obligations légales auxquelles est soumis le responsable de traitement ou d'autres principes. Mais ils sont à prendre en compte dans le traitement des données et le responsable de traitement doit toujours répondre quand une personne vient à les exercer. La Convention de Malabo a prévu quatre (4) droits pour les personnes concernées : droit à l'information (article 16), droit d'accès (article 17), droit d'opposition (article 18), droit de rectification et de suppression (article 19). Il convient de noter que certains Etats vont au-delà du cadre prévu par la Convention. Par exemple, le droit de suppression (ou d'effacement) est un droit autonome résultant de certains textes et n'étant pas nécessairement lié au droit de rectification. En outre, d'autres Etats ont ajouté dans leur loi, des droits qu'ils jugent nécessaires.



2.1 LES DROITS DES PERSONNES CONCERNÉES AU SÉNÉGAL

Droit à l'information

Le traitement des données à caractère personnel exige de la transparence de la part du responsable de traitement. Cette transparence nécessite que le responsable de traitement informe les personnes concernées des finalités du traitement, catégories de données traitées, destinataires des données, les mesures prises pour assurer la sécurité et la confidentialité des données et les droits que les personnes concernées peuvent exercer. Il est important de souligner que l'information doit être aisément accessible, compréhensible, claire et concise.

L'information des personnes concernées peut varier selon la nature du traitement.

Exemples :

- Une mention sur un site web.
- Un panneau comportant le pictogramme d'une caméra avec les informations relatives au responsable de traitement, aux finalités et à la durée de conservation pour un dispositif de vidéosurveillance.

Droit d'accès

Article 63 de la Loi 2008-12 : « Une copie des données à caractère personnel la concernant est délivrée à la personne concernée à sa demande ».

Le droit d'accès veut que toute personne justifiant de son identité puisse demander au responsable de traitement des informations lui permettant de connaître un traitement ou même de le contester. Le droit d'accès permet à une personne de savoir que ses données à caractère personnel sont traitées et d'en obtenir la communication dans un format compréhensible. Grâce au droit d'accès, une personne peut ensuite demander que ses données à caractère personnel traitées

soient rectifiées ou effacées. Le responsable de traitement peut s'opposer aux demandes abusives (article 66 de la Loi n° 2008-12).

Exemple : Amina, ancienne cliente d'une salle de sport pendant deux ans, exerce son droit d'accès afin d'obtenir communication des données à caractère personnel que l'établissement détient la concernant.

Droit de rectification

Article 69 de la Loi 2008-12 : « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexacts, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

Le droit de rectification permet de corriger les données inexacts dans un traitement ou de les compléter. Le droit de rectification peut résulter d'une nécessité de mise à jour.

Exemple : Avaga a déménagé. Il notifie ce changement à son fournisseur Internet pour que sa nouvelle adresse soit prise en compte. Le droit de rectification est également un corollaire du droit à l'erreur. En effet, toute personne dispose d'un droit à l'erreur. Ainsi, dans le cas où une personne commet une erreur dans le remplissage d'un document, il doit être en mesure de demander à le rectifier. De même, si une administration commet une erreur dans la saisie des données à caractère personnel d'un administré, ce dernier doit être en mesure de demander que ces données inexacts soient rectifiées.

Exemple : MADIBA Coulibaly Olunsegun, né le 02 juillet 1994 à Dakar au Sénégal est admis à

l'examen du BAC qu'il a passé en Côte d'Ivoire. Sur son attestation de diplôme, il est marqué MODIBO Couliboly Olunsegun né le 02 juillet 1994 à Dakar au Sénégal. Coulibaly peut faire valoir son droit de rectification afin d'obtenir correction et utiliser son diplôme de baccalauréat à toutes fins utiles.

Droit à l'effacement (ou de suppression)

Article 69 de la Loi 2008-12 : « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, (...) supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ». Le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé à l'effacement dans un délai d'un (1) mois après l'enregistrement de la demande.

Exemple : Maxime Evaglo, alors adolescent, a tenu des propos choquants sur un réseau social. Ayant depuis grandi et regrettant ses propos, il constate que, lorsqu'on effectue une recherche sur son nom en ligne, ces contenus restent parmi les premiers résultats affichés. Il peut exercer son droit de déréférencement afin que la société exploitant le moteur de recherche retire ces liens ou fasse en sorte qu'ils n'apparaissent plus prioritairement lors d'une recherche le concernant.

Droit d'opposition

Article 68 de la Loi 2008-12 : « Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Toute personne peut s'opposer à ce que ses données à caractère personnel fassent l'objet d'un traitement. Dans certains cas, la personne n'a pas besoin de justifier d'un motif légitime. C'est le cas, par exemple, de la prospection

directe.

Exemple : Je reçois régulièrement des offres publicitaires d'une entreprise. Je peux demander à cette entreprise de supprimer mes données à caractère personnel de sa liste de diffusion afin de ne plus recevoir ces offres. Dans cet exemple, l'entreprise supprime mes données à caractère personnel (adresse mail, numéro de téléphone, etc.) de sa liste de diffusion mais n'a pas à supprimer définitivement les données dont elle dispose me concernant dans le cadre du contrat qui me lie à la société. Ainsi, si j'exerce mon droit d'opposition s'agissant des appels de prospection d'un opérateur de téléphonie mobile, ce dernier cessera de m'appeler pour la finalité de prospection commerciale mais pourra conserver mes données s'il dispose d'une autre base légale, notamment celle d'une relation contractuelle relative à la gestion de mon compte d'abonné.



2.2 DROITS PRÉVUS AU SEIN D'AUTRES PAYS SUR LE CONTINENT AFRICAIN

Le droit à la portabilité (1) et le droit de ne pas faire l'objet de décisions individuelles automatisées (2) ne sont pas prévus par le droit sénégalais. Toutefois, ces droits sont reconnus dans d'autres réglementations, notamment au sein de l'Union européenne ainsi que dans plusieurs pays du continent africain.

Droit à la portabilité

Le droit à la portabilité permet d'obtenir communication de ses données à caractère personnel dans un format structuré et lisible par machine. Dans la mesure du possible, le responsable de traitement peut être amené à communiquer ces données à un autre responsable de traitement au profit de la personne concernée qui en fait la demande. Exemple : M. Tchalla est abonné chez un opérateur de téléphonie mobile. Il veut résilier son contrat avec cet opérateur tout en continuant à utiliser le même numéro de téléphone. En exerçant son droit à la portabilité, l'opérateur communique toutes les données à caractère personnel liées à son compte abonné (numéro de téléphone, messages, répertoire téléphonique...) au nouvel opérateur choisi par M. Tchalla.

Le droit de ne pas faire l'objet ou l'interdiction des décisions individuelles automatisées

Avec le développement des algorithmes de scoring et des systèmes automatisés, de nombreuses décisions impactant les personnes concernées sont prises sans contrôle humain.

Au niveau du continent africain :

- Article 14 §5 de la Convention de Malabo : "Aucune personne ne peut être concernée ni être soumise aux effets néfastes d'une décision

qui a des effets juridiques et qui est basée uniquement sur un traitement automatisé des données à caractère personnel pour évaluer certains aspects de sa personnalité."

- Article 35 §2 de l'Acte additionnel de la CEDEAO : "Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité".

Il en découle, en principe, une interdiction des décisions administratives ou privées prises à l'égard d'une personne physique et ayant pour effet de lui refuser un avantage ou la jouissance d'un droit, lorsque celles-ci reposent exclusivement sur les résultats d'un traitement automatisé visant à analyser son profil ou sa personnalité.

Elle comporte également une dimension assimilable à un « droit d'opposition » pour la personne concernée, laquelle peut refuser d'être soumise à ce type de décision. Ainsi, si un algorithme peut contribuer au processus décisionnel, il ne saurait, à lui seul, constituer l'unique fondement de la décision.

Exemple : Une banque se fonde sur le profil défini d'une personne (il ne rembourserait pas toujours ses crédits dans les conditions contractuelles) par un traitement automatisé de données à caractère personnel pour lui refuser un crédit. Une telle façon de procéder est en principe interdite. Mais même si elle est fondée sur le consentement de la personne concernée, dans les pays où cela est possible, celle-ci doit avoir le droit d'exiger une intervention humaine dans la prise de décision ou de la contester.

III. LA MISE EN OEUVRE DE CES DROITS

En pratique, un problème récurrent de qualification des demandes est observé dans le traitement des plaintes et demandes d'exercice des droits. Il arrive notamment qu'une personne concernée exerce son droit d'accès, tandis que le responsable du traitement procède, à tort, à l'effacement des données au lieu de fournir les informations sollicitées. Une telle confusion témoigne d'une compréhension encore imparfaite des droits consacrés par la législation relative à la protection des données à caractère personnel.

Dans ce contexte, un effort accru de sensibilisation apparaît nécessaire. Cette sensibilisation doit viser à la fois les responsables de traitement et les personnes concernées. Elle suppose une véritable acculturation au droit de la protection des données et aux textes en vigueur. Dans le cadre de la mise en œuvre du RGPD, la Commission nationale de l'informatique et des libertés (CNIL), autorité de protection des données personnelles en France, mène d'importantes actions de sensibilisation. À cet égard, des thématiques prioritaires sont définies chaque année, notamment en matière de contrôle et de respect des droits des personnes concernées.

Une telle approche pourrait constituer une source d'inspiration pour la CDP, notamment à travers la mise en place de campagnes annuelles de contrôle ciblées sur le respect effectif des droits des personnes concernées. Il ressort, en effet, qu'un déficit de connaissance et de mise en œuvre de ces droits persiste. Dès lors, la conduite de contrôles auprès des opérateurs, qu'ils soient publics ou privés, permettrait de rappeler que la loi consacre des droits précis et que leur application effective constitue une obligation légale. Ainsi, compte

tenu des mutations numériques actuelles et de l'évolution des législations sur le continent africain, le législateur pourrait envisager d'intégrer certains droits qui ne sont pas encore prévus par la législation locale, tels que le droit à la portabilité des données.

Le développement des systèmes d'intelligence artificielle, ainsi que la place croissante occupée par les grandes plateformes numériques, communément désignées sous l'acronyme GAFAM (Google, Apple, Facebook, Amazon et Microsoft) rendent indispensable le renforcement des garanties offertes aux personnes concernées. La consécration de ces droits apparaît donc particulièrement importante afin d'assurer un meilleur encadrement des traitements de données à caractère personnel et de préserver l'équilibre entre innovation technologique et protection des libertés individuelles.

Par ailleurs, des difficultés subsistent dans l'exercice effectif des droits existants, notamment en ce qui concerne l'accessibilité des mécanismes permettant leur mise en œuvre, comme les formulaires de contact ou les procédures de saisine. La CDP a déjà formulé plusieurs recommandations en ce sens et mené des actions de sensibilisation. Toutefois, il apparaît aujourd'hui nécessaire de renforcer la synergie entre les différents acteurs afin d'intensifier les efforts de sensibilisation, aussi bien à l'égard des personnes concernées que des organismes publics et privés. Une telle démarche permettrait d'améliorer l'effectivité des droits reconnus et de préparer le cadre juridique national aux défis posés par les transformations numériques en cours.

Comment agir ? La procédure en détail :

L'adresse unique pour agir : www.cdp.sn/plainte

Vous aurez 2 choix :

(i) La plainte : elle s'utilise lorsque la situation vous touche directement et personnellement. Exemple : une entreprise a utilisé vos données à caractère personnel sans consentement.

(ii) Le signalement : plus large, il permet de signaler un problème général (ex : une faille de sécurité sur un site même si ça ne vous a pas encore touché).

Lors d'un signalement, vous pouvez rester anonyme !

Autres moyens pour agir : appeler le +221 33 859 70 30 ou envoyer un mail à l'adresse suivante : contact.cdp@cdp.sn

IV. QUESTIONS/RÉPONSES DU WEBINAIRE

1) Comment s'organise la réponse aux droits des personnes concernées en cas de sous-traitance ?

En cas de recours à de la sous-traitance, la gestion des demandes d'exercice des droits des personnes concernées obéit à une organisation bien définie. En pratique, c'est le responsable du traitement qui reçoit les demandes d'exercice des droits (droit d'accès, de rectification, d'effacement, etc.). En effet, il constitue l'interlocuteur direct de la personne concernée, laquelle n'a généralement pas connaissance de l'ensemble de la chaîne de sous-traitance impliquée dans le traitement de ses données.

Toutefois, lorsque les données sont traitées par un ou plusieurs sous-traitants, la réponse à une demande peut nécessiter leur intervention. Dans ce cadre, des mécanismes de coopération sont prévus dans les contrats de sous-traitance. Ces contrats encadrent la relation entre le responsable du traitement et le sous-traitant et imposent à ce dernier plusieurs obligations, parmi lesquelles figure celle d'assister le responsable du traitement dans la gestion des demandes d'exercice des droits des personnes concernées. Cette obligation d'assistance peut également s'étendre aux demandes émanant des autorités de protection des données.

Ainsi, d'un point de vue contractuel, la coopération est organisée en amont. D'un point de vue pratique, lorsque le responsable du traitement reçoit une demande, il active ces mécanismes contractuels et sollicite le sous-traitant afin d'obtenir les informations nécessaires pour répondre de manière complète, exacte et dans les délais requis.





2) Comment les responsables de traitement s'assurent-ils qu'une personne ne maîtrisant pas forcément les outils numériques peuvent comprendre leurs droits ?

Dans les géographies africaines, il y a encore un certain retard en termes d'éducation et d'alphabétisation. Cette réalité pose directement la question de l'accessibilité concrète aux droits.

De manière classique et pratique, ce besoin d'information est généralement pris en charge à travers la mise en place de documents juridiques encadrant la relation avec les utilisateurs. Il s'agit notamment : des conditions générales d'utilisation, des politiques de confidentialité, des chartes d'utilisation, et plus largement des documents contractuels liant le prestataire de services numériques à ses clients. En effet, le socle juridique des interactions dans l'économie numérique repose essentiellement sur le cadre contractuel. Ces documents doivent préciser de manière claire et accessible : la finalité et la portée des traitements de données, les modalités de collecte, la nature des données traitées, le recours éventuel à des sous-traitants, les droits reconnus aux personnes concernées, ainsi que les modalités concrètes d'exercice de ces droits.

Une perspective intéressante pourrait consister à intégrer davantage les technologies vocales dans les services numériques en Afrique. Le développement croissant d'assistants vocaux, d'intelligences artificielles conversationnelles et de chatbots vocaux offre en effet des opportunités nouvelles pour répondre aux défis liés au déficit d'éducation numérique et au faible taux d'alphabétisation dans certaines zones. Ces outils permettent aux utilisateurs de dialoguer directement, par la voix, avec les fournisseurs de services numériques. L'interaction vocale apparaît souvent plus accessible, plus conviviale et plus efficace en termes d'impact, notamment pour les publics peu familiers avec les supports écrits ou les documents juridiques complexes.

Dans cette perspective, les responsables du traitement ainsi que les autorités de protection des données pourraient envisager la mise en place de cadres favorisant l'utilisation de ces technologies comme instruments de sensibilisation. Les technologies vocales, notamment lorsqu'elles sont proposées en langues nationales, pourraient constituer un levier important pour atteindre des populations éloignées des centres urbains ou disposant d'un accès limité à l'information juridique. En effet, une personne située dans une zone rurale ne dispose pas nécessairement des outils ou des compétences lui permettant de comprendre un contrat, des conditions générales d'utilisation ou une politique de confidentialité rédigés dans un langage juridique technique. En revanche, une information délivrée oralement, dans une langue comprise par l'utilisateur (dialecte local), via un assistant vocal fondé sur l'intelligence artificielle, pourrait significativement améliorer la compréhension des traitements de données et des

droits associés.

Une telle approche contribuerait ainsi au respect effectif du droit à l'information. Informer suppose non seulement de transmettre une information, mais également de s'assurer qu'elle est compréhensible. Le recours à des interfaces vocales adaptées aux réalités locales pourrait donc renforcer l'effectivité des droits des personnes concernées en matière de protection des données personnelles.

3) Existe-t-il un délai de mise en conformité pour les responsables de traitement, ou bien celui-ci est-il laissé à la libre appréciation de la CDP ?

Il n'existe pas de délai de mise en conformité à proprement parler. En effet, l'article 20 de la Loi 2008-12 prévoit de manière explicite l'obligation d'obtenir l'autorisation préalable de la CDP avant toute mise en œuvre d'un traitement de données à caractère personnel. La conformité doit donc, en principe, intervenir en amont du traitement. En pratique, il peut arriver que la CDP adopte une approche pragmatique en acceptant certaines régularisations. Toutefois, si les dispositions légales sont appliquées de manière stricte, aucun traitement ne devrait être mis en œuvre sans autorisation préalable.

4) Existe-t-il des données à caractère personnel qui restent indisponibles pour la personne concernée ?

En matière de droit d'accès, des limitations existent, la personne concernée dispose du droit d'obtenir l'accès à ses propres données à caractère personnel. Toutefois, ce droit ne saurait porter atteinte aux droits et libertés d'autrui. Autrement dit, la demande d'accès doit concerner uniquement les informations relatives à la personne physique qui l'exerce. Elle ne doit pas conduire à la divulgation de données à caractère personnel concernant des tiers.

La question se pose notamment dans le cadre des dispositifs de vidéosurveillance. Lorsqu'une personne exerce son droit d'accès à des images la concernant, il est fréquent que ces enregistrements comportent également des images d'autres individus. Dans ce type de situation, la pratique recommandée consiste à prendre des mesures techniques permettant de protéger les tiers, notamment par le caviardage ou le floutage des personnes apparaissant sur la vidéo, lorsque cela est techniquement possible.

Il n'existe pas, en principe, d'obligation systématique de saisir un service de police pour visionner les images, sauf dans des cas particuliers.

Dès lors que des moyens techniques permettent d'isoler les données relatives à la personne concernée sans porter atteinte aux droits des tiers, il convient en principe de donner suite à la demande d'accès.

Auteurs :

Jules Hervé YIMEUMI, Président d'Africa Data Protection

Kelly HAZAN, Avocate Data, Cyber, Tech & membre d'Africa Data Protection

Justin Yao KOUMAKO, Docteur en droit de la cybersécurité & membre d'Africa Data Protection

© 2026 AFRICA DATA PROTECTION. Tous droits réservés.