Cliniques Juridiques
Volume 8 – 2025

Accès au droit et protection des données personnelles

Natacha Gninou

Pour citer cet article : Natacha Gninou, « Accès au droit et protection des données personnelles », *Cliniques juridiques*, Volume 8, 2025 [https://cliniques-juridiques.org/?p=1131]

Accès au droit et protection des données personnelles

Natacha Gninou

1. En Afrique, la protection des données personnelles est devenue une préoccupation croissante en raison de la digitalisation que connaît le continent au fil des années. Durant ces 20 dernières années, de nombreux pays d'Afrique, comme d'autres dans le monde ont adopté des lois pour encadrer la collecte, le traitement et le stockage des données personnelles. Actuellement, près de 40 pays africain se sont dotés d'une telle loi, couvrant ainsi la majeure partie du continent. Parmi les pionniers, on compte le Cap- Vert avec la loi n°133-V-2001 [1], la Tunisie avec la loi organique n°2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel [2], le Sénégal avec la loi n°2008-12 du 25 janvier 2008 [3], le Maroc avec la loi 09-08 de 2009 [4]et le Bénin avec la loi N°2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin [5], qui avaient légiféré avant même l'avènement du RGPD [6]. Ces précurseurs ont ensuite fait évoluer leurs textes pour les aligner sur les normes modernes inspirées du RGPD. L'Afrique du Sud (loi POPIA 2013, effective depuis 2021), le Nigéria (Nigeria Data Protection Act de 2023, succédant à un règlement de 2019), le Ghana (Data Protection Act 2012), le Kenya (Data Protection Act 2019), la Côte d'Ivoire (loi de 2013, Autorité de protection rattachée à l'ARTCI), le Sénégal (loi de 2008 créant la Commission de Protection des Données Personnelles), le Togo (loi n°2019-014 du 29 Octobre 2019), le Burkina Faso (loi de 2004 révisée en 2021), ou encore l'Île Maurice (Data Protection Act mise à jour en 2017) [7].

2. D'autres pays francophones d'Afrique de l'Ouest ont emboîté le pas dans le cadre d'une initiative régionale. En 2010, la CEDEAO (Communauté économique des États de l'Afrique de l'Ouest) a adopté un Acte Additionnel visant à harmoniser les législations, ce qui a servi de base aux lois nationales au Bénin, Burkina Faso, Cap-Vert, Ghana, Niger, Sénégal dès 2013, rejoints par la Côte d'Ivoire peu après.

3. De même, la Communauté de développement d'Afrique australe (SADC) a proposé en 2013 une loi-type régionale pour guider ses membres, et plusieurs pays d'Afrique australe ont suivi avec leurs propres lois dans les années suivantes (ex. Zambie 2021, Zimbabwe 2021, Botswana 2018, Eswatini 2022, Lesotho 2012, Angola 2011…).

4. Ces pays africains se sont ainsi intéressés, dès le début des années 2000, aux enjeux de la protection des données personnelles [8]. Ces données essentielles au fonctionnement et à l'amélioration des nouvelles technologies sont aujourd'hui utilisées dans tous les secteurs

d'activités. De ce fait, les géants du secteur informatique investissent massivement afin d'avoir un maximum de données. Dans le secteur du droit en général et de la justice en particulier, les nouvelles technologies ont profondément transformé les pratiques, notamment en permettant un plus large accès à l'information juridique. Cela participe à l'amélioration de l'accès au droit. En effet, l'information juridique est disponible grâce aux différentes bases de données juridiques. Il n'est plus aujourd'hui nécessaire de passer de longues heures dans les bibliothèques pour trouver l'information nécessaire à la résolution de la difficulté qui se pose. Une simple requête dans un moteur de recherche juridique permet de ressortir une multitude de données.

5. Cependant, cela contraste avec les exigences de protection des données personnelles : l'ouverture numérique favorise l'accès au droit mais expose en même temps à des risques sérieux comme l'usurpation d'identité, la fraude financière, les atteintes à la réputation et le harcèlement en ligne. Ces risques découlent de violations de données dues à des cyberattaques, des erreurs humaines ou des divulgations involontaires, qui peuvent avoir des conséquences financières et juridiques importantes pour les individus comme pour les entreprises. Pour la protection des données personnelles. La diffusion de l'information juridique et particulièrement la diffusion des décisions judiciaires expose potentiellement les acteurs à une utilisation malveillantes de ces données.

6. Dans ce contexte, comment concilier la nécessité de rendre l'information juridique accessible à tous avec l'exigence de protection des données personnelles des acteurs concernés par cette diffusion ?

7. Le législateur togolais, confronté à la nécessité de protéger les données des utilisateurs, a adopté la loi 2019-014 du 29 octobre 2019 encadrant la protection des données. L'usage des nouvelles technologies dans les pratiques professionnelles africaines, bien qu'existant, est encore faible. Réfléchir à la protection des données personnelles dans le cadre de l'accès au droit reviendra à identifier d'une part, le cadre dans lequel l'accès aux droits est possible (I) avant d'envisager d'autre part la protection des données personnelles (II).

L'accès aux droits

8. L'accès au droit constitue l'un des fondements essentiels de l'État de droit. Il exprime la possibilité, pour chaque citoyen, de connaître ses droits, d'en comprendre la portée et de pouvoir les faire valoir devant les autorités compétentes. Dans une démocratie moderne, la connaissance du droit ne doit pas être réservée à une élite juridique ou administrative : elle doit être partagée par tous, comme condition de l'égalité réelle devant la loi.

9. Avec la révolution numérique [9], l'accès au droit a connu une transformation sans précédent. Les outils technologiques ont rendu les textes législatifs, la jurisprudence et la doctrine plus accessibles que jamais. Les portails juridiques, les sites gouvernementaux et les

bases de données ouvertes (open data) [10] permettent aujourd'hui à tout citoyen d'accéder gratuitement à l'information juridique, sans devoir franchir les barrières matérielles et intellectuelles qui limitaient autrefois cette accessibilité.

10. Historiquement, l'accès au droit se rattache au principe d'égalité devant la loi, proclamé dès 1789 par la Déclaration des droits de l'homme et du citoyen. Il est également consacré par les instruments internationaux, notamment par le Pacte international relatif aux droits civils et politiques [11] et la Charte africaine des droits de l'homme et des peuples [12], qui reconnaissent à toute personne le droit d'être entendue équitablement et de bénéficier d'un procès juste.

11. Mais l'accès au droit ne se limite pas à la justice au sens strict. Il englobe aussi la diffusion du savoir juridique et la compréhension des règles de droit. Le citoyen doit pouvoir connaître les textes qui s'appliquent à lui, comprendre les démarches administratives qu'il entreprend, et avoir les moyens d'obtenir conseil ou assistance juridique.

12. C'est dans cette optique que de nombreux États ont entrepris de mettre à disposition des portails d'accès au droit. En France, Légifrance a ouvert dès 2002 [13] l'accès à la législation et à la jurisprudence nationales. Dans l'espace africain, plusieurs initiatives similaires ont vu le jour : le site de l'OHADA met gratuitement à disposition les Actes uniformes et les arrêts de la Cour commune de justice et d'arbitrage (CCJA), contribuant ainsi à une meilleure harmonisation du droit des affaires.

13. Au Togo, le portail officiel du gouvernement (https://service-public.gouv.tg/) et les sites institutionnels du ministère de la Justice ou de l'ARMP (Autorité de régulation des marchés publics) jouent un rôle croissant dans la diffusion d'informations juridiques et administratives fiables. Ces outils participent à la construction d'un véritable espace de transparence normative.

14. La dématérialisation des procédures et la digitalisation des services publics ont profondément renouvelé les modalités d'accès au droit. Désormais, le citoyen peut accomplir de nombreuses démarches administratives en ligne, sans se déplacer. Les plateformes de e-justice ou de guichets uniques numériques simplifient les interactions entre les usagers et l'administration.

15. L'émergence d'outils d'intelligence artificielle contribue également à rendre le droit plus lisible. Les assistants juridiques automatisés, parfois sous forme de *chatbots* (robots conversationnels), permettent aux utilisateurs d'obtenir des explications accessibles sur leurs droits fondamentaux, leurs obligations fiscales ou leurs démarches judiciaires.

16. Cette dynamique s'inscrit dans une logique d'inclusion juridique : elle permet à un plus grand nombre de citoyens, notamment dans les zones rurales ou défavorisées, d'accéder aux

informations essentielles pour exercer leurs droits.

17. Toutefois, l'accès numérique au droit demeure inégalement réparti. La fracture numérique reste un obstacle majeur dans les pays en développement. Au Togo, malgré la progression du taux de pénétration d'Internet, une grande partie de la population, notamment en milieu rural, demeure exclue de cette transformation digitale. L'accès au droit ne peut être effectif que si les citoyens disposent des compétences numériques nécessaires pour naviguer dans cet environnement.

18. Un autre risque majeur tient à la désinformation juridique. Sur les réseaux sociaux ou certains sites non officiels, circulent des interprétations erronées du droit, pouvant induire les citoyens en erreur. Le numérique, en démocratisant la parole juridique, a aussi ouvert la porte à des discours non vérifiés, parfois manipulatoires.

19. Enfin, la numérisation massive du droit soulève des questions liées à la traçabilité des usagers. Chaque recherche, chaque requête, chaque consultation de document peut générer des métadonnées permettant de retracer le comportement juridique d'un individu. C'est ici que se manifeste la tension fondamentale entre accès au droit et protection des données personnelles, tension qui justifie une vigilance accrue des pouvoirs publics et des institutions spécialisées.

20. Si la société numérique a favorisé la transparence et la diffusion de l'information juridique, elle a également multiplié les risques d'atteinte à la vie privée. Les données personnelles circulent massivement, parfois sans le consentement ou la compréhension des personnes concernées. Les plateformes de services publics et les bases de données judiciaires ou administratives collectent, stockent des informations sensibles [14]. Or, la confiance du citoyen dans le système juridique repose sur la garantie que ses données seront protégées.

21. La protection des données à caractère personnel repose sur un corpus normatif désormais bien établi. Sur le plan international, le Règlement général sur la protection des données (RGPD) de l'Union européenne, adopté en 2016, a constitué une référence mondiale en posant les principes de licéité, de transparence, de minimisation et de sécurité des traitements de données.

22. Sur le continent africain, la Convention de Malabo adoptée par l'Union africaine en 2014 sur la cybersécurité et la protection des données personnelles a marqué une avancée majeure. Elle invite les États membres à mettre en place des législations nationales pour encadrer la collecte et le traitement des données.

23. Au Togo, cette recommandation a trouvé concrétisation à travers la loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel. Cette loi établit un cadre normatif complet : elle définit les données à caractère personnel, fixe les obligations des responsables de traitement, et reconnaît à toute personne physique le droit de s'opposer, de

rectifier ou de supprimer ses données.

24. La même loi a institué l'Instance de Protection des Données à Caractère Personnel (IPDCP), autorité administrative indépendante chargée de veiller au respect de la législation sur la protection des données. L'IPDCP constitue l'équivalent togolais de la CNIL française. L'IPDCP joue donc un rôle pivot dans la construction d'une culture nationale de la protection des données [15].

25. Selon l'Union Internationale des Télécommunications (UIT) [16], seulement 37% de la population africaine utilise internet [17]. Au Togo, bien que des efforts soient réalisés pour développer le numérique, notamment avec le projet de Code du numérique [18], la couverture internet reste faible dans plusieurs zones. L'accès aux bases de données juridiques et aux sites institutionnels diffusant les règles de droit applicable localement est donc difficile pour une grande partie des populations. Par ailleurs, l'accès aux outils numériques est marqué par les inégalités socio-économiques. Le coût élevé de la connexion, des ordinateurs et des smartphones exclut une partie de la population des dispositifs qui pourraient être mis en place afin d'assurer un accès au droit à travers les nouvelles technologies.

26. Ce contexte où l'accès à la technologie est limité n'empêche pas l'émergence de plateforme se fixant pour objectif de diffuser le droit. Depuis 2008 le site internet LegiTogo a été mis en ligne. Il se veut être le portail du droit togolais donnant un accès aux journaux officiels, aux textes applicables au Togo et à la jurisprudence. En plus de cette plateforme, le site du Tribunal de commerce de Lomé diffuse la jurisprudence commerciale togolaise [19]. Si de telles initiatives sont à saluer, elles ne doivent pas occulter la nécessité de protection des données exploitées dans un tel cadre particulièrement en ce qui concerne les décisions de justice qui sont publiées. En effet, la publication des décisions de justice doit être un point d'attention afin de garantir la protection des données publiées.

La protection des données personnelles

27. L'accès au droit et la protection des données apparaissent comme complémentaires dans leur finalité, mais entrent parfois en tension. La diffusion des décisions de justice illustre parfaitement cette tension. En effet, cette diffusion renforce la sécurité juridique et nourrit la recherche scientifique. La publicité de ces décisions peut même participer à augmenter la confiance des justiciables. Cependant, cette diffusion expose des données qui peuvent être sensibles (nom des parties, adresses, informations médicales ou patrimoniales, secret des affaires).

28. La publication des décisions de justice sans encadrement strict peut donc potentiellement porter atteintes à la protection des données des parties à un litige. Pour éviter la réalisation de ces risques, il convient d'adopter et de mettre en œuvre une gouvernance numérique intégrée. En l'absence de disposition encadrant spécifiquement la diffusion des décisions de justice au

Togo, l'autorité en charge de la protection des données (IPDCP) [20] devrait coopérer avec les institutions judiciaires en charge de la diffusion des décisions de justice pour définir des protocoles d'anonymisation et des standards de diffusion.

29. Si l'accès au droit suppose la diffusion libre et équitable de l'information juridique, il ne saurait se faire au détriment du droit fondamental à la protection des données personnelles. Le développement du numérique, en facilitant l'accès à la justice, la transparence administrative et la participation citoyenne, a parallèlement accentué la vulnérabilité des individus face à la collecte massive de leurs données. La protection des données apparaît alors comme une exigence démocratique, garantissant que l'ouverture de l'espace numérique ne se transforme pas en un terrain d'exploitation incontrôlée des identités personnelles.

30. L'ère numérique a profondément modifié la nature des relations entre l'individu, l'État et les opérateurs économiques. Les administrations publiques, les banques, les plateformes sociales ou les fournisseurs de services collectent, stockent et analysent quotidiennement des quantités considérables d'informations à caractère personnel : identité, coordonnées, données biométriques… Cette interconnexion généralisée, si elle facilite la gestion administrative et le commerce électronique, comporte des risques d'atteinte à la vie privée, de discrimination algorithmique [21] et d'usage abusif des données. La protection des données personnelles s'impose ainsi comme un impératif d'équilibre entre les bénéfices de la modernité technologique et la sauvegarde des droits fondamentaux de la personne humaine.

31. La particularité du dispositif togolais réside dans la création d'une autorité indépendante, l'Instance de Protection des Données à Caractère Personnel (IPDCP), qui doit jouer un rôle central dans la gouvernance numérique nationale. L'IPDCP contrôle la conformité des traitements, examine les plaintes des citoyens, émet des avis et autorisations, notamment pour les traitements sensibles comme ceux liés à la santé ou à la biométrie, et peut prononcer des sanctions administratives en cas de manquement.

32. L'action de l'IPDCP s'inscrit dans un écosystème institutionnel plus large. Plusieurs acteurs concourent à la protection effective des données. Les administrations publiques, en premier lieu, ont la responsabilité de sécuriser les bases de données qu'elles gèrent, notamment dans les secteurs de l'état civil, de la santé et de la fiscalité. Le secteur privé, en particulier les opérateurs de télécommunications, les banques et les sociétés de services numériques, est également soumis à des obligations de conformité. À leurs côtés, le législateur, les juridictions et la société civile participent à la consolidation d'une culture de la protection des données. Les ONG spécialisées et les médias jouent un rôle pédagogique essentiel dans la sensibilisation du grand public aux risques du numérique et aux réflexes de protection. Cette coopération entre acteurs publics et privés est indispensable, car la protection des données ne saurait être effective sans une conscience collective et partagée de son importance.

Notes

1. Loi n°133-V-2001 sur la protection des données personnels au Cap Vert.
2. Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, en Tunisie.
3. Loi n°2008-12 du 25 janvier 2008 sur la protection des données personnels au Sénégal.
4. Loi n°09 – 08 de 2009 portant protection des données personnelles au Maroc.
5. Loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin
6. Règlement Général sur la Protection des Données (RGPD), est une loi européenne qui encadre la collecte, le traitement et la sécurisation des données personnelles dans l'Union européenne. Entré en vigueur le 25 mai 2018, il vise à renforcer les droits des individus sur leurs informations personnelles, à responsabiliser les organisations traitant ces données, et à harmoniser les règles au niveau européen.
7. RGPD en Afrique : où en est-on en 2025 ? https://share.google/yOSMzui375QbUqKDt, page consulté le 30 Octobre 2025 à 16heures 02minutes.
8. État des lieux des législations sur la protection des données personnelles en Afrique | Africa Cybersecurity Magazine https://share.google/0F0N5ULfk7kBhbO8W, consulté ce 24 Août 2025.
9. Le point de départ de ce que l'on appelle généralement la révolution numérique correspond au passage des technologies électroniques mécaniques et analogiques aux technologies électroniques numériques dans le domaine du stockage, du transfert et de l'utilisation de l'information. Elle a commencé dans la deuxième moitié du 20e siècle avec l'adoption et l'essor des ordinateurs numériques et du stockage numérique de l'information, première étape vers la conception de systèmes informatiques plus avancés, capables de répliquer et d'automatiser numériquement des calculs mathématiques réalisés auparavant manuellement.
10. Open data (en français données ouvertes) sont des données numériques dont l'accès et l'usage sont laissés libres aux usagers, qui peuvent être d'origine privée mais surtout publique, produites notamment par une collectivité ou un établissement public. Elles sont diffusées de manière structurée selon une méthode et une licence ouverte garantissant leur libre accès et leur réutilisation par tous, sans restriction technique, juridique ou financière. Données ouvertes-Wikipédia https://share.google/BWO0AIi825oXdIUoR, page consulté le 30 octobre 2025 à 17heures 43minutes.
11. Article 14 du Pacte international relatif aux droits civils et politiques adopté à New York le 16 Décembre 1966
12. Article 7 de la charte africaine des droits de l'homme et des peuples adopté le 27 juin 1981 à Nairobi au Kenya et entrée en vigueur le 21 Octobre 1986.
13. Légifrance est instauré par l'arrêté du 6 juillet 1999 relatif à la création du site Internet Légifrance, arrêté modifié en octobre 2002 basé sur un décret d'août 2002 Légifrance – Wikipédia https://share.google/roNGbdmOuCbt5UC8G, page consulté le 30 Octobre 2025 à

18heures 42minutes.

14. Julien Rossi, *Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »*, Thèse de doctorat en Sciences de l'information et de la communication et Science politique, Julien Rossi, p.181.
15. L'Instance de Protection des Données à Caractère Personnel (IPDCP) est une autorité administrative indépendante créée par la loi n°2019-014 relative à la protection des données à caractère personnel. Elle a pour mission de veiller à ce que le traitement des données à caractère personnel soit conforme aux dispositions légales en vigueur, https://ipdcp.tg/, page consulté à 18heures 06 minutes.
16. Institutions spécialisées des Nations Unies pour les technologies de l'information et de la communication
17. Contre 90% de la population en Europe et en Amérique.
18. Vers l'élaboration d'un Code du numérique au Togo – Site officiel du Togo, République Togolaise https://share.google/u3po9Gc1hUSKLXg5v
19. Les décisions du tribunal, des cours d'appel et de la Cour Suprême en matière commerciale y sont publiés.
20. L'Instance de Protection des Données à Caractère Personnel (IPDCP) est une autorité administrative indépendante créée par la loi n°2019-014 relative à la protection des données à caractère personnel.
21. Université de génève, https://www.unige.ch/comprendre-le-numerique/archives/cas-pratiques/algorithmes-discriminatoires, Comprendre le numérique, consulté le 30 août 2025 à 18heures 21minutes.