Nubian Rights Forum c. Le Procureur général

Kenya, Afrique

Affaire Résolue
Renforce la liberté d'expression

DATE DE LA DECISION
30 janvier 2020

NUMERO DE L'AFFAIRE
Requêtes conjointes n° 56, 58 & 59 de 2019

ORGANE JUDICIAIRE
Cour de première instance

TYPE DE DROIT
Droit constitutionnel

PRINCIPAUX THEMES:
Vie privée, protection et conservation des données

ISSUE :
Loi ou action invalidée ou jugée inconstitutionnelle

MOTS CLES :
Droit à la vie privée, données biométriques

L'examen comprend :

- L'analyse de l'affaire
- Le sens de la décision
- La perspective globale
- L'importance de l'affaire

ANALYSE DE L'AFFAIRE

Résumé et issue

La Haute Cour du Kenya a estimé que la collecte de données ADN et GPS constituait une atteinte injustifiable au droit à la vie privée et était donc inconstitutionnelle, et que le cadre général de protection des données était insuffisant. Trois organisations non gouvernementales ont saisi la Cour après l'adoption d'amendements à la loi sur l'enregistrement des personnes qui eurent pour conséquence la création d'une base de données centrale d'informations biométriques et la mise en place d'un système de numéros d'identification uniques. La Cour a concédé la nécessité pour l'État de collecter et de détenir certaines informations biométriques, mais a estimé que les risques posés par la collecte de données ADN et GPS n'étaient pas compensés par ses avantages et n'étaient donc pas justifiables. Malgré l'adoption de la loi sur la protection des données pendant la procédure, la Cour a estimé que le cadre réglementaire régissant la collecte des données n'était pas suffisamment élaboré. Elle a donc déclaré que l'ensemble du système ne pourrait être mis en œuvre qu'après l'adoption d'un cadre réglementaire complet en matière de protection des données.

Les faits

Le 20 novembre 2018, la loi sur le droit statutaire (modifications diverses) n° 18 de 2018 a été promulguée au Kenya. La loi a modifié la loi sur l'enregistrement des personnes (Cap 107 des lois du Kenya) (la Loi) et a établi le système national intégré de gestion de l'identité (NIIMS), une source unique d'informations personnelles de tous les citoyens et étrangers résidant au Kenya. La section 9A(2) définit les fonctions du NIIMS comme suit :

> a) « créer, gérer, maintenir et exploiter un registre national de la population en tant que source unique d'informations personnelles de tous les citoyens kényans et des étrangers enregistrés résidant au Kenya ;
>
> b) attribuer un numéro d'identification national unique à chaque personne enregistrée dans le registre ;
>
> c) harmoniser, incorporer et collationner dans le registre les informations provenant d'autres bases de données des agences gouvernementales relatives à l'enregistrement des personnes ;

d) soutenir l'impression et la distribution, à des fins de collecte, de toutes les cartes d'identité nationales, des cartes de réfugiés, des certificats d'étrangers, des certificats de naissance et de décès, des permis de conduire, des permis de travail, des passeports et des documents de voyage à l'étranger, des cartes d'étudiant délivrées en vertu de la loi sur l'enregistrement des naissances et des décès, de la loi sur l'éducation de base, de la loi sur l'enregistrement des personnes, de la loi sur les réfugiés, de la loi sur la circulation routière et de la loi sur la citoyenneté et l'immigration du Kenya, ainsi que de toutes les autres formes de documents d'identification délivrés par le gouvernement et spécifiés par le secrétaire du Cabinet dans un avis publié dans la gazette ;

e) prescrire, en consultation avec les diverses autorités de délivrance concernées, un format de document d'identification permettant de saisir les diverses formes d'informations contenues dans les documents d'identification visés au paragraphe (d) aux fins de la délivrance d'un document unique, le cas échéant ;

f) vérifier et authentifier les informations relatives à l'enregistrement et à l'identification des personnes ;

g) rassembler les informations obtenues en vertu de la présente loi et les reproduire selon les besoins, de temps à autre ;

h) assurer la préservation, la protection et la sécurité de toute information ou donnée collectée, obtenue, maintenue ou stockée dans le registre ;

i) corriger les erreurs dans les détails de l'enregistrement, si une personne le demande ou de sa propre initiative, afin de s'assurer que l'information est exacte, complète, à jour et non trompeuse ; et

j) accomplir toute autre tâche nécessaire ou utile à l'exercice des fonctions prévues par la présente loi ».

Le terme « biométrique » a été défini dans la loi comme étant « des identificateurs ou des attributs uniques, notamment les empreintes digitales, la géométrie de la main, la géométrie du lobe de l'oreille, les motifs de la rétine et de l'iris, les ondes vocales et l'acide désoxyribonucléique sous forme numérique" et le terme « services de positionnement global »

a été défini comme étant « l'identificateur unique d'un emplacement géographique précis sur la terre, exprimé en caractères alphanumériques, qui est une combinaison de latitude et de longitude ».

Le Nubian Rights Forum - une organisation de défense des droits de l'homme qui protège les droits de la communauté nubienne du Kenya, - la Commission des droits de l'homme du Kenya et la Commission nationale des droits de l'homme du Kenya ont estimé que ces amendements violaient le droit à la vie privée prévu par l'article 31 de la Constitution. L'article 31 de la Constitution stipule que : « Toute personne a droit à la vie privée, ce qui inclut le droit de ne pas subir : (a) de fouille corporelle, ou de perquisition de son domicile ou de ses biens ; (b) de saisie de ses biens ; (c) de demande ou divulgation inutile d'informations relatives à sa famille ou à ses affaires privées ; (d) d'atteinte à la confidentialité de ses communications. »

Les organisations ont déposé des requêtes individuelles devant la Haute Cour du Kenya, qui ont ensuite été rassemblées. D'autres organisations, les Musulmans pour les droits de l'homme, le Centre Haki, la Law Society of Kenya et Inform Action se sont jointes aux requérants en tant que parties intéressées.

Les défendeurs étaient le Procureur général, le Secrétaire du Cabinet et le Secrétaire permanent de l'Intérieur et de la Coordination du Gouvernement national, le Directeur de l'Enregistrement national, le Secrétaire du Cabinet pour l'Information, la Communication et la Technologie, le Président de l'Assemblée nationale et la Commission de réforme du droit du Kenya. Les institutions, la Child Welfare Society of Kenya, Ajibika Society, Bunge La Mwananchi, International Policy Group et Terror Victims Support Initiative se sont jointes aux défendeurs pour s'opposer aux requêtes.

Avant la conclusion de l'affaire, le Parlement kényan a promulgué la loi 29 de 2019 sur la protection des données.

Aperçu de la décision

La juge Mumbi Ngugi, la juge Pauline Nyamweya et le juge Weldon Kipyegon Korir ont rendu le jugement. Les questions centrales à examiner étaient de savoir si les amendements limitaient le droit à la vie privée en permettant une collecte de données « excessive, intrusive et disproportionnée » ou si les garanties et les cadres de protection des données étaient insuffisants, et si les limitations étaient justifiables.

Les requérants ont souligné l'importance du droit à la vie privée et ont fait valoir qu'il « ne peut être dilué, enfreint et/ou entravé par l'État sans justification appropriée » [paragraphe 709]. Ils ont fait valoir que la collecte de données ADN et GPS était intrusive et inutile car il n'y avait pas de restrictions légales sur la conservation des données et le gouvernement kenyan n'avait pas fourni d'explication sur les raisons pour lesquelles la collecte de ces données était nécessaire. Les requérants ont fait valoir que les données étaient collectées sans le consentement des sujets et que la loi n'était pas claire quant à la finalité de la collecte des données. En outre, les requérants ont fait valoir qu'il y avait un risque que des tiers non autorisés aient accès aux informations personnelles stockées dans le système NIIMS et que, sans garanties solides, l'utilisation des technologies biométriques peut « faciliter la discrimination, le profilage et la surveillance de masse » [paragraphe 712]. En ce qui concerne la vie privée des enfants, les requérants ont fait valoir que, puisque la Loi stipule que ses dispositions s'appliquent aux personnes âgées de plus de 18 ans, elle ne s'applique tout simplement pas aux enfants et ne peut être utilisée pour recueillir des données biométriques d'enfants. Ils ajoutent qu'en tout état de cause, aucune garantie n'est prévue pour réglementer l'utilisation des données des enfants et que rien ne prouve que la collecte de données biométriques puisse prévenir les crimes contre les enfants. Les requérants ont fait valoir qu'il n'y avait pas de lois de protection des données en place pour empêcher les données de tomber entre des mains non autorisées et qu'il était « impératif que des normes techniques et juridiques appropriées soient formulées pour garantir la sécurité du système d'identification numérique proposé et la confidentialité des données personnelles recueillies » [paragraphe 829]. Les requérants ont fait valoir que l'État n'avait pas fourni de preuves justifiant que l'objectif de la loi était si important qu'il portait atteinte au droit au respect de la vie privée ou que les moyens adoptés étaient le seul moyen possible d'atteindre l'objectif législatif, et qu'aucune preuve n'avait été fournie sur la manière dont le NIIMS contribuerait à la prévention de la criminalité - l'un des objectifs déclarés du système - ou que des mesures moins restrictives avaient été envisagées.

Les défendeurs publics ont fait valoir que la collecte de données biométriques, y compris de données GPS, était une pratique courante dans le monde et qu'il n'y avait pas d'attente raisonnable en matière de respect de la vie privée en ce qui concerne les empreintes digitales et les scans de l'iris. L'État a soutenu que la collecte des données biométriques des enfants contribuait à la protection des enfants contre la traite et à la réalisation des droits fondamentaux des enfants, et que la collecte des données ADN était autorisée au Kenya et permettait de déterminer la paternité d'un enfant. Toutefois, l'État a fait valoir que, dans la pratique, aucune donnée ADN ou GPS n'était collectée au Kenya, mais que cette collecte était, en théorie, importante. L'État a maintenu qu'il existait un cadre juridique suffisant en matière de protection des données et a fait valoir que la constitutionnalité d'une loi ne peut être déterminée par l'absence de cadres législatifs ou réglementaires. L'État a réaffirmé que l'objectif de la loi était de créer un système national intégré de gestion de l'identité et qu'il s'agissait d'un objectif légitime de l'État qui ne portait pas une atteinte disproportionnée au droit à la vie privée.

La Cour a divisé les questions concernant le droit à la vie privée en quatre sections : (a) la question de savoir si les renseignements recueillis étaient « excessifs, intrusifs et disproportionnés par rapport aux objectifs déclarés du NIIMS » ; (b) la question de savoir s'il y avait atteinte à la vie privée des enfants ; (c) la question de savoir « s'il existe des garanties juridiques et des cadres de protection des données suffisants pour les renseignements personnels recueillis dans le cadre du NIIMS » ; et (d) la question de savoir si les modifications constituaient une « limitation déraisonnable et injustifiable du droit à la vie privée » [paragraphe 705].

La Cour a procédé à une analyse de la nature du droit au respect de la vie privée et de la manière dont les juridictions comparées ont traité les questions de confidentialité de l'information. Elle a noté que l'article 31 protégeait ce droit et » protège contre des atteintes spécifiques à la vie privée, notamment la révélation inutile d'informations relatives à des affaires familiales ou privées » [paragraphe 742]. La Cour s'est référée à l'affaire Bernstein c. Bester NO de la Cour constitutionnelle sud-africaine, qui a été suivie dans les affaires Ebrahim c. Ashleys Kenya, Kenya Legal and Ethical Network on HIV & AIDS (KELIN) c. Cabinet Secretary Ministry of Health, et Tom Ojienda t/a Tom Ojienda & Associates Advocates c. Ethics and Anti-Corruption Commission, et à la protection du droit donnée par la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques,

la Convention européenne des droits de l'homme et la Commission africaine des droits de l'homme et des peuples. Elle a décrit l'étendue du droit comme étant « non définissable » et comme étant « un ensemble ou un continuum de droits qui ont des justifications diverses » [paragraphe 748]. L'aspect du droit en cause dans la présente affaire était le droit au respect de la vie privée en matière d'information, qui comprend le droit de contrôler ses propres informations, et la Cour a adopté la définition de l'affaire KELIN selon laquelle le droit « protège contre la révélation inutile d'informations relatives aux affaires familiales ou privées d'un individu, [...] protège le cœur même de la sphère personnelle d'un individu et envisage fondamentalement le droit de vivre sa propre vie avec un minimum d'interférence [...] [et] restreint la collecte, l'utilisation et la divulgation d'informations privées » [paragraphe 751]. En se référant à l'affaire sud-africaine Mistry c. Interim National Medical and Dental Council of South Africa, la Cour a noté que lorsque la vie privée informationnelle est en cause, la Cour doit déterminer si la collecte de l'information était intrusive, si l'information portait sur des aspects intimes de la vie de l'individu, si l'information était utilisée à une fin autre que celle pour laquelle elle avait été fournie et si l'information était largement diffusée.

La Cour a reconnu que, comme elles contiennent des informations sur une personne, la protection des données biométriques relève de l'article 31 et que les données recueillies dans le cadre du NIIMS constituent des informations personnelles. Elle a noté que ce point était important car « la qualification de données biométriques comme personnelles a des conséquences importantes en ce qui concerne la protection et le traitement de ces données et, en tant que telle, entraîne un risque de violation du droit à la vie privée en cas de mesures de protection inadéquates » [paragraphe 760]. La Cour a accepté la catégorisation des « données sensibles » établie dans le Règlement général sur la protection des données (RGPD) de l'Union européenne, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, et la loi sur la protection des données nouvellement introduite, et a estimé que les données biométriques et génétiques « doivent être protégées contre tout accès non autorisé, et que l'accès à ces données devrait également être limité par des pratiques de sécurité des données suffisantes conçues pour empêcher toute divulgation non autorisée et toute violation des données » [paragraphe 762].

La Cour a estimé qu'au moment où le NIIMS a été introduit, il n'y avait aucune obligation pour une personne de consentir à ce que ses données biométriques soient collectées, et que par conséquent, bien que la loi sur la protection des données exige désormais le consentement et

permette à une personne de s'opposer au traitement de ses données, les amendements autorisaient la collecte de données sans consentement. La Cour s'est référée au document de travail sur la biométrie de l'organe consultatif de l'Union européenne sur la protection des données et de la vie privée pour affirmer que la collecte de certaines données biométriques autorisée par le NIIMS était intrusive et a donné l'exemple de la collecte d'informations sur l'ADN à l'insu du sujet. En ce qui concerne la collecte de données GPS, la Cour s'est référée à l'affaire United States c. Antoine de la Cour suprême des États-Unis en notant que les amendements nécessitaient une « réglementation plus détaillée et plus stricte de l'utilisation des coordonnées GPS » afin d'empêcher leur utilisation abusive [paragraphe 771].

En conséquence, la Cour a estimé que la collecte de données biométriques et GPS constituait la collecte d'informations personnelles et sensibles qui nécessitaient une protection et obligeaient l'État à adopter des mesures de protection des données.

La Cour a examiné la question de savoir si la collecte des données personnelles était nécessaire. Se référant à l'affaire indienne Puttaswamy c. Union of India (II) et au document de travail sur la biométrie du groupe de travail sur la protection des données de l'article 29, la Cour a noté que la collecte de données biométriques a pour but de vérifier l'identité d'une personne et que, pour que la collecte soit autorisée, les données biométriques recueillies doivent être universelles, uniques et permanentes [paragraphe 778]. La Cour a estimé que la plupart des données collectées dans le cadre du NIIMS répondaient à ces critères, mais que la collecte de données ADN n'y répondait pas. La Cour a fait référence à l'affaire S et Marper c. Royaume-Uni 30562/04 de la Cour européenne des droits de l'homme pour conclure que la collecte de données ADN dans le cadre du NIIMS constituait une violation du droit à la vie privée. Elle a également estimé que la nécessité de collecter des données GPS n'était pas évidente, en particulier compte tenu des risques d'atteinte à la vie privée que présente la collecte de ces données.

En conséquence, la Cour a estimé que la collecte de données ADN et GPS était « intrusive et inutile » et inconstitutionnelle, mais que la collecte d'autres données biométriques ne constituait pas une violation de l'article 31. La Cour a reconnu que l'objectif central du NIIMS était l'autorisation et la vérification des individus, ce qui nécessitait la création d'une base de données centrale, et a estimé que les avantages du NIIMS « sont dans l'intérêt public et ne sont pas inconstitutionnels » [paragraphe 790].

Dans son examen suivant, la Cour a évalué si les processus du NIIMS violaient le droit à la vie privée des enfants. La Cour a estimé que les raisons invoquées par l'État pour justifier l'enregistrement des enfants dans le cadre du NIIMS - la capacité de lutter contre le terrorisme, la traite des enfants et le travail des enfants, ainsi que de protéger les droits constitutionnels des enfants, notamment à l'éducation, à la nutrition, au logement et aux soins de santé, ainsi que contre les abus - étaient « raisonnables et louables » [paragraphe 809]. En conséquence, la Cour a estimé que la collecte des données biométriques des enfants était constitutionnelle. Toutefois, la Cour a estimé que le libellé et la structure de la loi étaient tels que le NIIMS ne s'appliquait pas aux enfants.

Le troisième volet de son examen consistait à déterminer si les garanties juridiques et les cadres de protection des données étaient suffisants. La Cour a accepté les arguments de Privacy International sur les risques d'exclusion, de violation des données et de « détournement d'usage » (la collecte de données pour une finalité autre que celle prévue initialement) posés par les systèmes d'identité biométriques, et a noté que l'accès non autorisé et l'utilisation abusive peuvent entraîner « la discrimination, le profilage, la surveillance des personnes concernées et l'usurpation d'identité » et que le stockage central signifie que les personnes concernées n'ont aucun contrôle sur l'utilisation de leurs données [paragraphe 880]. Se référant au rapport sur la confidentialité des données du Haut-Commissaire des Nations unies aux droits de l'homme, la Cour a déclaré que « tous les systèmes biométriques, qu'ils soient centralisés ou décentralisés, et qu'ils utilisent une technologie fermée ou ouverte, nécessitent une politique de sécurité forte et des procédures détaillées sur leur protection et leur sécurité, conformes aux normes internationales » [paragraphe 883]. La Cour a examiné le RGPD, les principes de l'ONU sur la protection des données personnelles et la vie privée, les principes de l'OCDE sur la vie privée et la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles. La Cour a constaté que la loi sur la protection des données avait intégré « la plupart des principes applicables en matière de protection des données », mais qu'elle ne s'appliquait pas à la loi sur l'enregistrement des personnes - la législation pertinente en l'espèce - et que les règlements nécessaires à la loi sur la protection des données n'avaient pas été publiés.

La Cour a également examiné si le régime de protection était suffisant pour protéger les données informationnelles des enfants, et a estimé que la loi elle-même ne prévoyait aucune protection et que, bien que la loi sur la protection des données ait introduit une certaine

protection, l'absence de dispositions de protection spécifiques aux enfants rendait le cadre législatif inadéquat en ce qui concerne la protection des données des enfants.

En conséquence, la Cour a estimé que « le cadre juridique relatif aux opérations du NIIMS est inadéquat et présente un risque pour la sécurité des données qui seront collectées dans le NIIMS » [paragraphe 885].

Enfin, la Cour a examiné si les limitations du droit à la vie privée - par la collecte de données ADN et GPS et en raison des insuffisances du cadre de protection des données - étaient inutiles, déraisonnables et injustifiables. Selon la Constitution kenyane, un droit ne peut être limité qu'en vertu de l'article 24, qui exige que la limitation soit conforme à la loi et « seulement dans la mesure où la limitation est raisonnable et justifiable dans une société ouverte et démocratique fondée sur la dignité humaine, l'égalité et la liberté, compte tenu de la nature du droit ou de la liberté fondamentale » [paragraphe 912]. La Cour a souligné que les tribunaux doivent évaluer l'objectif et l'importance de la limitation et déterminer s'il existe des moyens moins restrictifs pour atteindre cet objectif.

La Cour a estimé que la collecte de données ADN et GPS sans garanties ni procédures appropriées était injustifiable. Elle a également estimé que le cadre défini par la loi était incomplet, qu'il ne créait pas un cadre global pour la collecte de données à caractère personnel et qu'il n'était donc pas clair et sans ambiguïté. En conséquence, la Cour a estimé que le processus était injustifiable et inconstitutionnel.

La Cour a déclaré inconstitutionnels les articles exigeant la collecte de données ADN et GPS, et a estimé que l'État pouvait mettre en œuvre le système NIIMS « à condition qu'un cadre réglementaire approprié et complet sur la mise en œuvre du NIIMS soit conforme aux exigences constitutionnelles applicables » [paragraphe 1047].

SENS DE LA DECISION

Issue : Renforce la liberté d'expression

En soulignant la nécessité d'une législation appropriée et d'un cadre réglementaire complet pour la collecte de données biométriques, les juges ont limité les pouvoirs arbitraires du gouvernement de violer le droit à la vie privée des individus.

PERSPECTIVE GLOBALE

Sommaire des références

Normes, lois ou jurisprudences nationales

- Kenya, Coalition for Reforms & Democracy & autres c. République du Kenya& 10 autres, requête n° 628 of 2014 regroupée avec les requêtes n° 630 de 2014 & 12 de 2015
- Kenya, Trusted Society of Human Rights Alliance c. Procureur général et autres Haute Cour, Requête n° 229 de 2012
- Kenya, Okuta c. Procureur général et 2 autres [2017] eKLR
- Kenya, Geoffrey Andare c. Procureur général et 2 autres, Requête n° 149 of 2015, [2016] eKLR
- Kenya, Alai c. Attorney General n° 147 of 2016
- Kenya, Kenya Human Rights Commission c. Communications Authority of Kenya [2018] eKLR
- Ken., Kenya Legal and Ethical Network on HIV & AIDS (KELIN) c. Cabinet Secretary Ministry of Health [2016] eKLR
- Ken., Tom Ojienda t/a Tom Ojienda & Associates Advocates c. Ethics and Anti-Corruption Commission [2016] eKLR
- Ken., Ebrahim c. Ashleys Kenya [2016] eKLR

Lois internationales et/ou régionales pertinentes

- UE, Règlement (UE) 679/2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).
- CEDH, S. et Marper c. Royaume Uni [GC], Plainte n° 30562/04 et 30566/04 (2008)

Autres normes, lois ou jurisprudences nationales

- Can., R. c. Oakes, [1986] 1 S.C.R. 103
- Can., R. c. Big M Drug Mart Ltd., [1985] 1 S.C.R. 295
- Inde, Justice Puttaswamy (Retd) & Anr c. Union of India & Ors (2017), 10 SCC 1
- Afrique du Sud, Mistry c. Interim National Medical and Dental Council of South Africa, 1998 (4) SA 1127 (CC)
- Afrique du Sud, Bernstein c. Bester, (CCT23/95) [1996] ZACC 2

- Jam., Robinson c. e Procureur général de la Jamaïque, Plainte n° 2018 HCV01788
- États-Unis, United States c. Antoine 565 US (2012)

IMPORTANCE DE L'AFFAIRE

La décision établit un précédent contraignant ou persuasif dans sa juridiction.

DOCUMENTS OFFICIELS DE L'AFFAIRE

- Jugement (Anglais)

Rapports, analyses, et articles de presse :

- **La Haute Cour du Kenya suspend la mise en œuvre du système d'identification biométrique**
  https://ohrh.law.ox.ac.uk/high-court-of-kenya-suspends-implementation-of-biometric-id-system/