Puttaswamy c. Union of India (II)

Inde, Asie et Asie-Pacifique

Affaire Résolue
Restreint la liberté d'expression

MODE D'EXPRESSION
Expression non-verbale

DATE DE LA DECISION
26 septembre 2018

NUMERO DE L'AFFAIRE
(2019) 1 SCC 1

ORGANE JUDICIAIRE
Cour suprême (cour d'appel en dernier recours)

TYPE DE DROIT
Droit constitutionnel

PRINCIPAUX THEMES:
Vie privée, protection et conservation des données

ISSUE :
Loi ou action maintenue

MOTS CLES :
Vie privée, Données biométriques, Données personnelles

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

Cinq juges de la Cour suprême de l'Inde statuant ensemble ont confirmé la validité constitutionnelle du Targeted Delivery of Financial and Other Subsidies, Benefits, and Services Act, 2016 (« Aadhaar Act ») tout en annulant certaines dispositions de la loi. Aadhaar, un numéro d'identification à 12 chiffres délivré par la Unique Identification Authority of India (« UIDAI ») aux résidents de l'Inde, permet un processus plus efficace de délivrance de plusieurs régimes de protection sociale aux résidents de l'Inde. Ce système a été contesté principalement pour atteinte aux droits fondamentaux garantis par les articles 14, 19 et 21 de la Constitution indienne. La Cour a estimé que l'utilisation d'Aadhaar aux fins des programmes d'aide sociale était constitutionnelle car la loi Aadhaar a résisté aux tests constitutionnels de l'objectif légitime de l'État, de la nécessité et de la proportionnalité. Elle a également estimé que, puisque l'objectif de la loi était de créer une identification unique permettant aux bénéficiaires méritants d'accéder à des subventions ou à des services (dont les dépenses sont prélevées sur le Fonds consolidé de l'Inde), la loi Aadhaar a été valablement adoptée en tant que loi de finances. La Cour a également confirmé la liaison obligatoire d'Aadhaar avec les cartes PAN, tout en déclarant que la liaison obligatoire d'Aadhaar avec les comptes bancaires était inconstitutionnelle et disproportionnée. Plus important encore, la Cour a estimé que les entreprises privées ne pouvaient pas exiger des citoyens qu'ils fournissent leur numéro Aadhaar pour la prestation de services.

Les faits

En 2012, le juge KS Puttaswamy a déposé une un recours en justice contestant la validité constitutionnelle du projet Aadhaar, qui visait à constituer une base de données sur l'identité personnelle et les informations biométriques de chaque Indien. Aadhaar est un numéro d'identification à 12 chiffres délivré par la *Unique Identification Authority of India* (« UIDAI ») aux résidents de l'Inde et est lié à plusieurs programmes d'aide sociale, permettant un processus plus efficace de prestation de services et évitant les faux bénéficiaires (« programme Aadhaar »). Ce programme visait à créer une base de données sur l'identité personnelle et les informations biométriques de chaque Indien et avait inscrit plus de 1,1 milliard de personnes en Inde en 2018.

Conceptualisé en 2006 pour un avant-projet d'identification des familles en dessous du seuil de pauvreté, le dispositif Aadhaar a connu de multiples versions avant d'être lancé à l'échelle nationale par le biais d'une action administrative en l'an 2009. Le 25 mars 2016, le dispositif Aadhaar a reçu une sanction juridique avec la promulgation de la loi de 2016 sur la prestation ciblée de subventions,

avantages et services financiers et autres « Aadhaar Act »). En vertu de cette loi, l'UIDAI a été créée en tant qu'organe statutaire pour développer la politique, la procédure et les systèmes d'émission de numéros Aadhaar aux individus et également pour effectuer l'authentification conformément aux dispositions de la loi. Tous les résidents de l'Inde devaient soumettre des informations démographiques (nom, date de naissance et adresse) et biométriques (photographie, empreinte digitale et scan de l'iris) au moment de l'inscription à une agence d'inscription (« processus d'inscription »). Notamment, l'agence d'inscription est une entité privée. Les données sont stockées dans le Central Identities Data Repository (« CIDR ») qui est une base de données centralisée contenant tous les numéros Aadhaar, les détails démographiques et les informations biographiques de ces individus.

Bien que le système soit destiné à faciliter la réception de subventions, de prestations et de services sur présentation d'une preuve de possession d'un numéro Aadhaar, une exigence supplémentaire pour les personnes qui demandent un tel avantage est de se soumettre à une authentification à chaque fois, en soumettant non seulement un numéro Aadhaar mais aussi en fournissant des informations biométriques à l'agence. À la réception de ces informations, l'agence (appelée « entité requérante » dans la loi) est tenue d'envoyer la demande à l'UIDAI, qui procède ensuite à la confirmation de l'identité de la personne (« processus d'authentification »). Une fois le processus terminé avec succès, la personne est autorisée à recevoir la prestation.

Compte tenu de la portée de la loi et de son impact sur la vie privée des résidents, le système a fait l'objet d'un examen public approfondi, ce qui a conduit à un certain nombre d'actions en justice contre lui. La première de ces affaires a été déposée en 2012 par le juge KS Puttaswamy (un juge retraité de la Haute Cour de l'État indien du Karnataka) et Pravesh Khanna (un avocat), qui ont déposé un recours en justice contestant la validité constitutionnelle du projet Aadhaar, principalement au motif d'une violation du droit à la vie privée en vertu de la partie III de la Constitution indienne.

En réponse à la proposition du gouvernement de rendre le système Aadhaar obligatoire pour accéder aux services et avantages gouvernementaux, plusieurs autres recours ont également été déposés, contestant certains aspects du système. La contestation a d'abord été faite devant un conseil de trois juges de la Cour suprême. Dans son ordonnance du 11 août 2015, le jury a noté que les normes et la compilation des données biométriques démographiques par le gouvernement ont été remises en question principalement au motif qu'elles violent le droit à la vie privée. Cependant, le procureur général a fait valoir au nom de l'Union indienne que la Constitution indienne n'accorde pas de protection spécifique au droit à la vie privée. Il s'est fondé sur les observations faites dans l'affaire M.P. *Sharma c. Satish Chandra* (un jury de huit juges) et *Kharak Singh c. Uttar Pradesh* (un jury de cinq juges). Cependant, les requérants ont contesté le fait que ces deux jugements étaient fondés sur des principes établis en 1950 dans l'affaire *A.K. Gopalan c. State of Madras (« Gopalan »)*, qui a été infirmée par un

jury de onze juges dans l'affaire *Rustom Cavasji Cooper c. Union of India* (« Cooper ») en 1970. Dans l'affaire Cooper, le jury a estimé que les droits fondamentaux ne devaient pas être interprétés comme des droits distincts et sans rapport entre eux, confirmant ainsi l'opinion dissidente exprimée dans l'affaire Kharak Singh. Cette décision a également servi de base à des décisions ultérieures prises par des jurys plus restreints de la Cour suprême, qui ont expressément reconnu le droit à la vie privée.

Face à cette situation difficile et compte tenu de l'importance de la question, un renvoi à un jury plus large a été jugé approprié pour décider s'il existait un « droit fondamental protégé par la Constitution » en matière de vie privée. C'est dans ce contexte qu'un jury de cinq juges a été mis en place par une ordonnance du 11 août 2015. Le 18 juillet 2017, un jury constitutionnel a estimé qu'un jury plus large de neuf juges serait plus à même de décider si la position consignée par la Cour suprême dans les affaires M.P Sharma et Kharak Singh (c'est-à-dire qu'il n'existe pas de droit fondamental à la vie privée en vertu de la Constitution indienne) était bien fondée. Le jury de neuf juges dans *Puttaswamy c. Union of India (« Puttaswamy* I ») a donné une réponse unanime et a déterminé que le droit à la vie privée fait partie des droits fondamentaux qui peuvent être retracés aux articles 14, 19 et 21 de la Constitution indienne. Suite à l'arrêt *Puttaswamy I*, la Cour suprême a renvoyé l'affaire pour une audience finale devant le jury de cinq juges dans cette affaire.

Aperçu de la décision

Le jury de cinq juges de la Cour suprême de l'Inde a rendu l'arrêt. La question principale qui se posait à la Cour était d'évaluer si les dispositions de la loi Aadhaar violaient le droit fondamental à la vie privée en vertu des articles 14, 19 et 21 de la Constitution indienne.

En vertu de la Constitution indienne, l'article 14 garantit le droit à l'égalité, l'article 19 garantit le droit à la liberté de parole, d'expression et de réunion, et l'article 21 garantit le droit de toute personne à la vie et à la liberté individuelle. Le jugement dans *Puttaswamy I* a garanti le droit à la vie privée comme une partie intrinsèque du droit à la vie et à la liberté personnelle en vertu de l'article 21 de la Constitution indienne. Dans le cadre de la loi Aadhaar de 2016, le chapitre II traite de l'inscription, exigeant que chaque résident obtienne le numéro Aadhaar en soumettant ses informations démographiques et biométriques (article 3). Le chapitre III traite de « l'authentification », l'article 7 stipulant que la preuve d'un numéro Aadhaar sera nécessaire pour bénéficier de certaines subventions, prestations et services, etc. D'autres articles importants de la loi comprennent le chapitre IV, qui traite de la création de l'UIDAI et le chapitre VI, qui définit la sécurité des informations et des enregistrements d'authentification des personnes, ainsi que la restriction du partage des informations biométriques. Notamment, les informations collectées et stockées sont traitées comme un « enregistrement électronique » et des « données ou informations personnelles sensibles » en vertu de

l'article 30 de la loi. L'article 33 de la loi impose également une interdiction à l'UIDAI de collecter, conserver ou maintenir toute information relative au « but de l'authentification » sauf (a) dans les circonstances où une ordonnance d'un tribunal non inférieur à celui d'un juge de district pour divulguer ces informations a été faite (paragraphe 1) et (b) lorsqu'il devient nécessaire de divulguer l'information dans l'intérêt de la sécurité nationale (paragraphe 2). L'article 57 de la loi prévoit que la loi Aadhaar n'empêche pas l'utilisation d'un numéro Aadhaar pour établir l'identité d'un individu à quelque fin que ce soit.

Divers textes réglementaires ont également été élaborés en vertu de la loi, notamment (a) le règlement Aadhaar (inscription et mise à jour), 2016, pour collecter les informations démographiques de tous les individus ; (b) le règlement Aadhaar (authentification), 2016, pour prévoir des dispositifs d'authentification et saisir, enregistrer et conserver les informations biométriques ; (c) le règlement Aadhaar (sécurité des données), 2016, pour assurer la sécurité des informations ; et (d) le règlement Aadhaar (partage des informations), 2016, pour réglementer le partage des informations démographiques collectées par l'UIDAI.

En vertu d'une majorité unanime dans *Puttaswamy I*, la Cour suprême de l'Inde avait déclaré le droit à la vie privée comme un droit fondamental. Sur la base de ce postulat, les requérants ont fait valoir devant la Cour que le système Aadhaar était intrusif et « forçait » une personne souhaitant s'inscrire à divulguer ses principales informations biométriques et à les fournir à une entité privée chargée de collecter ces données. Il en résulte un risque sérieux d'utilisation abusive d'informations privées vitales, en particulier pendant le processus d'authentification, lorsqu'une personne non seulement divulgue ses informations biométriques à une entité requérante, mais divulgue également à cette entité le but et la nature de la transaction qu'elle est censée effectuer à ce moment-là. Étant donné que les informations relatives à la personne et à ses transactions étaient reliées à une base de données centrale, cela présentait un risque de surveillance de l'État en permettant à ce dernier de dresser le profil des citoyens, de suivre leurs déplacements, d'évaluer leurs habitudes et d'influencer leur comportement. En outre, il n'y avait aucune garantie de protection des données à quelque niveau que ce soit. Le système avait la capacité de générer la « mort civile » d'un individu en désactivant son identifiant Aadhaar. Vu sous cet angle, le système a rompu l'équilibre et faussé la relation entre le citoyen et l'État, octroyant à l'État une domination totale de l'individu.

De manière plus générale, les contestations ont été faites pour les motifs suivants :

La surveillance : Au motif que le projet a créé une architecture pour une surveillance de masse omniprésente, permettant à l'État de localiser la personne qui cherche à s'authentifier et lui permettant de construire des profils complets d'individus par la convergence des données [en s'appuyant sur

Kharak Singh c. État de l'UP (1964) 1 SCR 332, U. S. c. Jones 132 S.Ct. 945 (2012) (États-Unis), *Zakharov c. Russie* (2015) Requête n° 47143/2006 (CEDH), *Digital Rights Ireland Ltd. c. Ministre de la communication, des ressources marines et naturelles* [2014] All ER (D) 66 (Apr) et *S et Marper c. Royaume-Uni* (2008) CEDH 1581].

Violation du droit à la vie privée au titre de l'article 19 : Au motif que le projet violait le droit fondamental à la vie privée en ce qui concerne les informations personnelles démographiques et biométriques collectées, stockées et partagées ; portait atteinte à l'autonomie et à la dignité de l'individu ; et violait le droit à la vie privée informationnelle en exigeant des individus qu'ils se soumettent à une authentification obligatoire par le biais de la plateforme Aadhaar sans possibilité d'utiliser un autre mode d'identification. Plus précisément, les requérants ont également affirmé que la loi permettait la collecte de données sans distinction concernant tous les aspects d'une personne (données biométriques, détails démographiques, enregistrements d'authentification, métadonnées liées à la transaction) même si ces données n'ont aucun lien avec l'objet supposé des subventions, violant ainsi le principe de minimisation des données.

Violation du principe de l'autorité limitée du gouvernement : au motif que le projet a perturbé le principe de la souveraineté du peuple avec une autorité limitée du gouvernement qui est la caractéristique fondamentale de la Constitution, en favorisant un État totalitaire. En rendant Aadhaar obligatoire pour divers services publics, le projet a eu un effet dissuasif sur l'autonomie du peuple.

Législation déguisée : les requérants ont affirmé que la loi n'a pas suivi la procédure constitutionnelle et qu'elle a été déguisée en « Loi de finance » (un projet de loi qui ne concerne que la fiscalité nationale, les fonds publics ou les prêts), ce qui rend la loi nulle en raison de son caractère de législation de circonstance. En outre, l'objectif du projet en tant qu'"exercice d'identification" était illégal et ultra vires.

Violation de l'article 14 et de l'article 21 : La procédure adoptée par les défendeurs pour promulguer la loi Aadhaar a violé le droit à l'égalité en vertu de l'article 14 et le droit à la vie et à la liberté individuelle en vertu de l'article 21 car (a) il n'y avait pas de consentement éclairé au moment de l'inscription et le modèle était intrusif, excessif et disproportionné, (b) les données collectées et téléchargées dans le CIDR n'ont pas été vérifiées par un fonctionnaire du gouvernement désigné par l'UIDAI, (c) la procédure a permis à l'agence d'inscription ainsi qu'à l'entité requérante de capturer, stocker et utiliser à mauvais escient les informations biométriques et démographiques sans que l'UIDAI n'ait aucun contrôle sur cette utilisation et (d) l'architecture d'Aadhaar, par sa nature même, étant probabiliste, a entraîné l'exclusion de cas authentiques. La loi viole également le droit à la

protection contre l'auto incrimination [déclaré comme une composante de la liberté individuelle dans *Selvi & Ors. c. État du Karnataka* (2010) 7 SCC 263].

En réponse à cette requête, les défendeurs ont principalement invoqué trois motifs. Premièrement, seules des données biométriques minimales sont stockées dans le CIDR et il n'y a pas de collecte « d'autres » données concernant la religion, la caste, la tribu, la langue, les enregistrements de droits, le revenu ou les antécédents médicaux d'une personne. Deuxièmement, puisque les informations biométriques dans l'écosystème d'inscription sont transmises sous forme cryptée, l'inscription et le processus d'authentification sont infaillibles, l'UIDAI se contentant de comparer les données biométriques et ne stockant ni ne recevant aucune autre information concernant le lieu, le but ou la nature de la transaction. Enfin, les informations sont collectées en silos et restent archivées hors ligne, les données envoyées aux systèmes d'identification biométrique automatique (« ABIS ») dans les centres d'inscription étant complètement anonymisées pour garantir la sécurité et la confidentialité des données.

L'opinion majoritaire a été rendue par le juge Sikri, avec laquelle le juge en chef de l'Inde Misra et le juge Khanwilkar ont exprimé leur accord. Le juge Ashok Bhushan a rendu une opinion séparée mais concordante. Le juge Chandrachud a émis une opinion dissidente. Ces opinions sont résumées ci-dessous :

Opinion majoritaire de Sikri J., le juge en chef de l'Inde Misra J. approuvée par le juge Khanwilkar :

L'auteur de l'opinion majoritaire a commencé par analyser la jurisprudence sur les différentes facettes de la vie privée, affirmant trois aspects du droit fondamental à la vie privée : (i) l'intrusion du corps physique d'un individu ; (ii) la vie privée informationnelle ; et (iii) la protection de la confidentialité du choix. Par la suite, la Cour a cherché à catégoriser diverses approches dans la formulation de la vie privée, en classant la vie privée sur la base du préjudice (c'est à dire la vie privée étant un concept de ressemblance familiale), des intérêts (c'est à dire la protection de l'intimité du repos, l'intimité du sanctuaire et des décisions intimes) et de l'agrégation de droits (c'est à dire non limitée à un droit fondamental mais associée à plusieurs autres droits) [paragraphe 168]. La Cour a ensuite posé la question suivante : quelle est la portée du droit à la vie privée et dans quelles circonstances un tel droit peut-il être limité ?

Déclarant que toute action de l'État doit être examinée à la lumière des articles 14, 19 et 21 de la Constitution indienne, la Cour a noté qu'une restriction à un droit doit également satisfaire au critère de contrôle judiciaire en vertu (a) des motifs spécifiés à l'article 19(2) de la Constitution (principalement

dans l'intérêt de la souveraineté et de la sécurité de l'État, de l'ordre public, de la décence, de la moralité, etc.) et (b) la restriction doit être raisonnable. Sur ce dernier point, la Cour a cherché à appliquer diverses normes, y compris l'application du test du but légitime et la doctrine de la proportionnalité. Plus particulièrement, la Cour a également cherché à savoir si elle devait appliquer la norme de « l'examen strict » ou celle du « caractère juste, équitable et raisonnable » pour déterminer la légalité de la loi. Ces aspects sont analysés en détail ci-dessous :

Doctrine de la proportionnalité :

Selon le principe de proportionnalité, une action de l'Etat qui violerait le droit à la vie privée doit être testée selon trois paramètres : (a) l'action doit être sanctionnée par la loi ; (b) l'action proposée doit être nécessaire dans une société démocratique pour un but légitime ; et (c) l'étendue de cette ingérence doit être proportionnelle à la nécessité de cette ingérence. Après avoir exposé la compréhension de la proportionnalité dans diverses juridictions, la Cour a établi que quatre sous-éléments de la proportionnalité doivent être satisfaits, à savoir

(a) une mesure restreignant un droit doit avoir un but légitime (étape du but légitime) ;

(b) elle doit être un moyen approprié pour atteindre ce but (étape de l'adéquation ou du lien rationnel);

(c) il ne doit pas exister d'autre solution moins restrictive mais tout aussi efficace (étape de la nécessité) ; et

(d) la mesure ne doit pas avoir un impact disproportionné sur le titulaire du droit (étape de la pondération). [p. 125]

En déterminant l'application du principe de proportionnalité en ce qui concerne le stade de la nécessité (élément « c »), la Cour, s'appuyant sur l'arrêt *Puttaswamy I*, a adopté l'analyse de David Bilchitz pour déclarer que les éléments suivants peuvent être adoptés pour préserver un rôle significatif mais pas indûment strict pour le stade de la nécessité. Premièrement, il faut identifier une série d'alternatives possibles à la mesure employée par le gouvernement. Deuxièmement, l'efficacité de ces mesures doit être déterminée individuellement ; le critère ici n'est pas de savoir si chaque mesure respective réalise l'objectif gouvernemental au même degré, mais plutôt si elle le réalise d'une « manière réelle et substantielle ». Troisièmement, il faut déterminer l'impact des mesures respectives sur le droit en cause. Enfin, il faut juger globalement si, à la lumière des conclusions des étapes précédentes, il existe une alternative préférable. Ce faisant, la Cour a également souligné l'importance d'avoir un objectif légitime suffisamment important pour justifier de passer outre un droit protégé par la Constitution.

En appliquant le test de proportionnalité, la Cour a estimé que (a) puisque la loi Aadhaar sert à atteindre un but légitime de l'État (objectif légitime de l'État), la restriction du droit à la vie privée est justifiée, (b) puisqu'il n'existe aucune autre mesure « moins restrictive » pouvant atteindre le même objectif, la loi Aadhaar a également passé le cap de la nécessité (étape de la nécessité), (c) il existe un lien rationnel entre les dispositions de la loi et les objectifs qu'elle cherche à atteindre (étape du lien rationnel), et (d) la loi Aadhaar établit un juste équilibre entre les droits fondamentaux concurrents (c. à d.) (étape de la pondération).

En ce qui concerne la pondération, la majorité a examiné la question à deux niveaux : (i) si « l'intérêt légitime de l'État » garantissait une « adaptation raisonnable » et (ii) si la pondération de deux droits fondamentaux concurrents, le droit à la vie privée d'une part et le droit à la nourriture, au logement et à l'emploi d'autre part, a été effectuée. Sur le premier point, la Cour a déclaré qu'il y avait une intrusion minimale dans la vie privée et que la loi était encadrée de manière étroite pour atteindre l'objectif. En ce qui concerne le second point, la Cour a analysé la relation entre le droit à la vie privée de l'individu et le droit à la vie du même individu en tant que bénéficiaire, bien que les arguments de la Cour ne soient pas clairs sur ce point, car elle passe du conflit entre les deux droits individuels ci-dessus aux droits entre les individus et « dans l'intérêt public général ». La Cour a estimé qu'étant donné que les informations collectées au moment de l'inscription et de l'authentification sont minimes, la pondération au premier niveau était respectée. Au deuxième niveau, c'est-à-dire lorsqu'il s'agit de mettre en balance deux droits fondamentaux concurrents [à savoir la dignité sous la forme de l'autonomie (vie privée informationnelle) et la dignité sous la forme de l'assurance d'un meilleur niveau de vie pour le même individu], la Cour a estimé que l'inscription à Aadhaar des personnes défavorisées et marginalisées de la société leur permettait de bénéficier des programmes d'aide sociale du gouvernement et que, par conséquent, le programme garantissait la dignité de ces personnes.

Surveillance de l'État :

Sur la question de savoir si le projet Aadhaar a créé ou avait tendance à créer un régime de surveillance, la Cour a cherché à répondre à deux questions : (a) si l'architecture du projet Aadhaar permet à l'État de créer un régime de surveillance ; et (b) s'il existe des dispositions adéquates en matière de protection des données pour s'en protéger [p. 235]. A la question (a), la Cour a répondu par la négative, notant que le processus d'inscription et d'authentification était fortement réglementé dans la mesure où il était sécurisé et rendait ainsi très difficile la création du profil d'une personne simplement sur la base des informations biométriques et démographiques stockées dans le CIDR. La Cour a également récapitulé les mécanismes de sécurité pour constater que des garanties adéquates étaient intégrées dans la conception du système [p. 153].

À la question (b), après avoir examiné la jurisprudence des États-Unis, de l'Union européenne et de l'Inde sur le sujet, la Cour est arrivée à une réponse similaire à celle de la question (a), estimant que le programme Aadhaar était largement compatible avec les principes de la protection des données. En ce qui concerne plus particulièrement l'argument de la minimisation des données, la Cour a conclu que le principe de minimisation des données était respecté puisque l'article 2(k) de la loi Aadhaar interdit la collecte d'informations sensibles telles que la race, la religion, la caste, la tribu, l'origine ethnique, la langue, les dossiers de prestations, les revenus ou les antécédents médicaux. En outre, l'article 32(3) de la loi conjointement avec le règlement 26 des Règles d'authentification interdit également à l'UIDAI de collecter, de stocker ou de conserver, directement ou indirectement, toute information concernant l'objectif de l'authentification.

Il convient de noter que la majorité a également estimé que, dans certains cas, les dispositions de la loi n'étaient pas compatibles avec les principes de la protection des données. Il s'agit notamment de :

(a) les règlements 26 et 27 de la réglementation Aadhaar (authentification) de 2016 (imposant le stockage des métadonnées pendant une période de sept ans) : la Cour a convenu avec les requérants que les données pouvaient être conservées pendant une période déraisonnablement longue. Il n'y avait pas non plus de limitation de finalité car il était possible que les informations d'identité collectées pour une finalité en vertu de la loi puissent être utilisées pour toute autre (nouvelle) finalité. Dans l'intérêt du droit du citoyen à l'effacement des données et du droit à l'oubli, la Cour a donc interprété la loi comme ne conservant que les « métadonnées de traitement » (c'est-à-dire limitées au moment de l'authentification, à l'entité requérante et à la réponse oui/non aux demandes d'authentification) pour une période limitée à six mois.

(b) L'article 33 de la loi Aadhaar de 2016 (autorisant la divulgation d'informations, y compris les enregistrements d'identité et d'authentification, si elle est ordonnée par un tribunal, ainsi que la divulgation dans l'intérêt de la sécurité nationale) : l'article 33(1) de la loi a également été lu, en précisant qu'une personne, dont on cherche à divulguer les informations, doit avoir la possibilité d'être entendue. La Cour a déclaré inconstitutionnel l'article 33(2), qui permet le partage d'informations pour des raisons de sécurité nationale.

(c) L'article 57 de la loi Aadhaar de 2016 (autorisant les parties privées à mandater Aadhaar) : en vertu de l'article 57 de la loi, l'État, une personne morale ou toute personne avaient le droit de recourir au dispositif d'authentification et d'accéder aux informations dans le cadre du CIDR. La Cour a estimé que cette disposition allait à l'encontre du principe de consentement éclairé au moment de l'inscription et l'a donc jugée inconstitutionnelle.

Droit à la vie privée selon la Constitution indienne :

Sur la question de savoir si la loi Aadhaar violait le droit à la vie privée, les requérants ont fait valoir qu'il n'y avait pas d'intérêt impérieux de l'État à connaître les détails du lieu et de l'heure pendant le processus d'authentification. En outre, alors que la loi a été conçue comme un droit volontaire à établir l'identité, les actions de l'exécutif et des entités privées (en exigeant Aadhaar comme condition préalable pour bénéficier de services, de subventions et d'avantages) ont rendu la possession d'Aadhaar obligatoire de facto - cette forme d'exclusion pour les sections marginalisées a violé le droit fondamental à l'égalité en vertu des articles 14 et 21 de la Constitution. L'atteinte à la vie privée n'était pas non plus justifiée au regard du principe de proportionnalité.

Les défendeurs ont fait valoir, d'autre part, qu'il n'y avait pas d'attente raisonnable de respect de la vie privée en ce qui concerne les informations d'identité recueillies en vertu de la loi Aadhaar à des fins d'authentification et que, par conséquent, l'article 21 n'était pas applicable [p. 318]. Sur la base de ce qui précède, les tests de proportionnalité d'intrusion minimale et de contrôle strict n'étaient pas applicables. Les défendeurs ont également fait valoir que l'intérêt légitime de l'État auquel répond la loi Aadhaar est la prévention des fuites et de la dissipation des subventions et des prestations sociales couvertes par l'article 7 de la loi Aadhaar, et que sur cette base, elle satisfait au critère de proportionnalité.

La Cour a observé, en s'appuyant sur *Puttuswamy I*, que l'article 21 ne protège que les questions pour lesquelles il existe une attente raisonnable de respect de la vie privée. La majorité a testé ce principe sur deux fronts : premièrement, le ou les individus revendiquant un droit à la vie privée doivent établir que leur revendication implique une inquiétude quant à un préjudice susceptible de leur être infligé en raison de l'acte allégué ; deuxièmement, cette inquiétude ne doit pas être déraisonnable [p. 330]. Elle a également estimé que le triple test établi pour juger du caractère raisonnable de l'atteinte à la vie privée était réalisé, car (a) le système Aadhaar était soutenu par la loi, c'est-à-dire la loi Aadhaar, (b) il servait un objectif légitime de l'État, à savoir assurer la distribution ciblée de subventions aux bénéficiaires, grâce à une identification précise et (c) il était proportionné.

En particulier, en considérant la dignité humaine comme une facette de la vie privée, la Cour a fait remarquer ce qui suit :

« Il s'agit de la pondération de deux facettes de la dignité d'un même individu. Si, d'une part, le droit à l'autonomie personnelle fait partie de la dignité (et du droit à la vie privée), une autre partie de la

dignité du même individu consiste à mener une vie digne (ce qui est également une facette de l'article 21 de la Constitution). Par conséquent, dans un scénario où l'État met en place des programmes d'aide sociale qui s'efforcent de donner une vie digne en harmonie avec la dignité humaine et où, dans le processus, un certain aspect de l'autonomie est sacrifié, l'équilibre entre les deux devient une tâche importante qui doit être accomplie par la Cour. En effet, il ne peut y avoir d'intrusion indue dans l'autonomie sous prétexte de conférer des avantages économiques ». [p. 540]

Il est important de noter que la majorité a identifié toute l'architecture du système comme étant « unique » et éliminant tout risque de duplication. Elle a estimé que « une fois que les informations biométriques sont stockées et que la carte Aadhaar est délivrée sur cette base, elles restent dans le système auprès de l'Autorité. Chaque fois qu'il y aurait une deuxième tentative d'inscription à Aadhaar et qu'à cette fin la même personne donnerait ses informations biométriques, celles-ci seraient immédiatement comparées aux mêmes informations biométriques déjà présentes dans le système et la deuxième demande serait rejetée ». [p. 529]

Loi de finance et législation déguisée

Il est utile de rappeler que la loi Aadhaar a été adoptée en tant que « loi de finance », ce qui la rend vulnérable à la validité juridique en raison de la doctrine de la législation déguisée. En vertu de l'article 110(3) de la Constitution indienne, la décision du président du Lok Sabha est considérée comme définitive en cas de litige sur le fait qu'un projet de loi soit un projet de loi de finances ou non. S'appuyant sur cette disposition, les défendeurs ont fait valoir que la décision du Président n'était pas soumise à un contrôle judiciaire. En outre, étant donné que les dépenses pour « la prestation ciblée de subventions, d'avantages et de services » sont encourues à partir du Fonds consolidé de l'Inde, l'intention législative et l'objet de la loi étaient valables, car le « cœur et l'âme de la loi », en vertu de l'article 7, vise à identifier et atteindre les bénéficiaires pour ces subventions, avantages et services. Les requérants ont soutenu que certaines dispositions de la loi ne relevaient pas de l'article 110 et qu'en l'absence d'une clause de divisibilité, l'ensemble de la loi devait être déclarée nulle. En ce qui concerne la justiciabilité du président, les requérants ont également affirmé que la Cour était habilitée à décider si la décision du président était constitutionnellement correcte.

Sur cette question, la majorité a d'abord examiné si le projet de loi répondait aux exigences de l'article 110(1). Elle a estimé que l'article 7 était la disposition centrale de la loi Aadhaar et que, étant donné que l'authentification basée sur Aadhaar était exigée par l'article 7 de la loi pour la réception d'une subvention, d'un avantage ou d'un service et que ces subventions, avantages et services provenaient du Trésor indien, la disposition satisfaisait aux conditions de l'article 110 de la Constitution [p. 483-484]. En outre, d'autres dispositions de la loi [c'est-à-dire les articles 23(2)(h), 54(2)(m) et 57 de la loi

Aadhaar] permettaient à l'Autorité de spécifier les modalités d'utilisation d'Aadhaar dans un but précis, à savoir pour fournir ou bénéficier de diverses subventions, prestations et services. Par conséquent, la Cour a estimé que le projet de loi Aadhaar devait être présenté comme un projet de loi de finances. Elle n'a pas abordé les autres arguments des requérants après s'être prononcée sur la question préliminaire, à savoir si la déclaration du président selon laquelle le projet de loi est un projet de loi de finances peut faire l'objet d'un contrôle judiciaire ou non et si une disposition qui ne concerne pas un projet de loi de finances est divisible ou non.

Exclusion, gouvernance limitée et autres questions connexes :

Sur l'aspect spécifique de l'exclusion, la Cour a également noté l'argument du requérant selon lequel le processus d'authentification était de nature probabiliste - conduisant souvent à l'échec de l'authentification dans les cas authentiques. Cependant, elle a rejeté ce raisonnement, estimant au contraire que l'article 7 de la loi était une disposition habilitante, et qu'en cas d'échec, une telle personne serait autorisée à établir son identité par d'autres moyens. La Cour a également pris acte de la déclaration du Procureur général de l'Inde selon laquelle aucune personne méritante ne se verrait refuser le bénéfice d'un programme en cas d'échec de l'authentification.

Sur la question de la gouvernance limitée, les requérants avaient affirmé que le projet Aadhaar était néfaste à la gouvernance limitée, au constitutionnalisme et à la confiance constitutionnelle. Ces arguments étaient fondés sur le fait que l'architecture d'Aadhaar est constitutionnellement intrusive, qu'elle menace l'autonomie des individus et qu'elle a tendance à créer un régime de surveillance. Cependant, la Cour a considéré que ces arguments étaient excessifs - combinés à la lecture des dispositions litigieuses de la loi, elle a estimé que le régime légal régirait globalement les citoyens et a rejeté les arguments sur cette base.

La Cour a également mis en garde - en réponse à l'argument des requérants selon lequel l'expression « prestations » était ouverte et permettait aux défendeurs d'inclure dans son champ d'application tout type d'activité gouvernementale au nom du bien-être des communautés - que les « prestations » devaient être celles qui sont propres aux programmes d'aide sociale pour lesquels des ressources doivent être prélevées sur le Fonds consolidé de l'Inde.

Il convient de noter que la majorité a également analysé l'impact du système sur les enfants et a estimé que, bien qu'il soit essentiel que les enfants aient le consentement de leurs parents/tuteurs pour s'inscrire au système, à l'âge de la majorité, les enfants qui sont inscrits à Aadhaar avec le consentement de leurs parents auront le droit de quitter Aadhaar [p. 401]. En ce qui concerne l'admission des enfants

à l'école, l'exigence d'Aadhaar ne serait pas obligatoire car il ne s'agit ni d'un service ni d'une subvention.

En outre, le jugement majoritaire a également analysé la constitutionnalité de diverses dispositions spécifiques de la loi Aadhaar, et a jugé que la majorité de ces dispositions étaient valides [p. 402-442]. Comme indiqué précédemment, il a toutefois invalidé l'article 57 dans la mesure où il permet aux intervenants privés de rendre Aadhaar obligatoire pour les résidents.

En ce qui concerne d'autres lois, notamment l'article 139AA de la loi de 1961 relative à l'impôt sur le revenu (qui exige de lier le numéro Aadhaar à d'autres formes d'identité telles que le numéro de compte personnel), la Cour a estimé que la loi satisfaisait aux critères applicables, à savoir l'existence de la loi, les intérêts légitimes de l'État et la proportionnalité. En ce qui concerne la règle 9 relative à la prévention du blanchiment d'argent (tenue de registres) des Règles de 2005 (reliant le numéro Aadhaar au compte bancaire), la Cour a toutefois estimé que la disposition ne répondait pas au critère de proportionnalité et qu'elle violait donc le droit à la vie privée d'une personne, qui s'étend aux coordonnées bancaires. La majorité a également jugé inconstitutionnelle la circulaire du 23 mars 2017 imposant la liaison du numéro de téléphone mobile avec Aadhaar.

Opinion dissidente du juge Chandrachud :

Le juge Chandrachud était en désaccord avec l'hypothèse de base de la majorité sur le caractère unique du système Aadhaar, déclarant que le caractère unique des données biométriques était relatif et demeurait une hypothèse " sans preuve irréfutable " [p. 779]. Il a noté que la loi soulevait d'importantes préoccupations en matière de protection de la vie privée, dont notamment les suivantes :

(a) l'absence de consentement lors de l'inscription et de l'authentification, car avant la promulgation de la loi Aadhaar, aucune obligation n'était imposée aux bureaux d'enregistrement ou aux agences d'inscription pour (i) obtenir le consentement éclairé des résidents avant d'enregistrer leurs données biométriques, (ii) les informer de la manière dont les données biométriques seraient stockées et utilisées et (iii) de l'existence de garanties adéquates pour sécuriser les données ;

(b) l'étendue de l'information divulguée lors de l'authentification et du partage des informations biométriques de base ;

(c) la portée élargie des informations biométriques ; et

(d) l'efficacité douteuse du modèle biométrique (y compris le vol d'identité).

Plus précisément, le juge Chandrachud a accordé une grande importance à l'autodétermination en tant que facette essentielle de l'article 21 et a également souligné l'incohérence entre le modèle biométrique déployé par Aadhaar et le droit à l'anonymat des citoyens. Sur ce dernier point, étant donné que l'anonymat est au cœur du sentiment de liberté et d'autonomie d'une personne, l'utilisation généralisée de la biométrie porte atteinte au droit de rester anonyme. Dans l'ensemble, le juge Chandrachud a estimé que le cadre Aadhaar violait les normes essentielles relatives à la confidentialité des informations, à l'autodétermination et à la protection des données.

En ce qui concerne la proportionnalité, tout en acceptant la décision de la majorité selon laquelle l'article 7 de la loi Aadhaar répond à un objectif légitime de l'État, le juge Chandrachud a contesté le fait que le système ait résisté au test de proportionnalité. Compte tenu de l'absence d'obligation de rendre des comptes, de l'absence d'objectifs adéquats en matière de traitement des exceptions, de l'absence de règles claires et de la nature non limitative de l'article 7 (comme le montre la définition de « prestation » à l'article 2(f) et de « service » à l'article 2(w)), le système a été considéré comme excessivement disproportionné. L'opinion minoritaire a observé que la loi Aadhaar et ses règlements d'application étaient dépourvus de la procédure par laquelle une personne peut accéder aux informations relatives à son dossier d'authentification. L'architecture d'Aadhaar aurait dû intégrer dans la loi, mais ne l'a pas fait, la création d'une autorité de contrôle indépendante. Il est également important de noter le paragraphe 255 du jugement où il mentionne :

Il n'y a pas d'antinomie entre le droit à la vie privée et les objectifs légitimes de l'État. Une atteinte à la vie privée doit être proportionnelle et soigneusement adaptée à la réalisation d'un objectif légitime. Bien que le droit à l'alimentation soit un droit important et que sa promotion soit une obligation constitutionnelle de l'État, le droit à la vie privée ne peut pas simplement et automatiquement s'y soumettre. Aucun but légitime de l'État ne peut être autorisé au prix d'une atteinte à un droit fondamental sans passer le test de constitutionnalité. [p. 919]

Cumulativement, le juge Chandrachud a estimé que le système Aadhaar était capable de détruire différentes identités constitutionnelles, qu'il était inadéquat pour protéger l'intégrité des données personnelles, le droit à l'autodétermination informationnelle et les droits attribuables à la trilogie vie privée-dignité-autonomie. Étant donné que la technologie biométrique, qui est au cœur du programme Aadhaar, est de nature probabiliste, ce qui entraîne des échecs d'authentification, les échecs d'authentification ont conduit à la négation des droits et des prestations légales. Le programme a également causé une intrusion injustifiée dans les libertés fondamentales garanties par la Constitution indienne, tandis que l'exclusion financière causée par les erreurs d'authentification basées sur Aadhaar a également violé le droit à la dignité de l'individu.

Sur la question de la surveillance, il a observé que le système permettait de relier différentes bases de données (gérées par l'État ou des entités privées) - de cette manière, le « numéro Aadhaar [est devenu] l'élément unificateur central qui relie le téléphone portable aux données de géolocalisation, la présence et les déplacements d'une personne à un compte bancaire et aux déclarations d'impôt sur le revenu, la consommation d'aliments et le mode de vie aux dossiers médicaux » [p. 903]. Par conséquent, il a estimé que le fait de relier Aadhaar à différentes bases de données comporte le risque d'être profilé dans un système qui pourrait être utilisé à des fins commerciales. Il est également possible d'influencer les modèles de comportement des individus, en affectant leur vie privée et leur liberté. Le profilage des individus pourrait alors être utilisé pour créer des corrélations entre des vies humaines, qui ne sont généralement pas reliées entre elles. Puisque Aadhaar devient un pont entre des silos de données discrètes - ce qui permet à toute personne ayant accès à ces informations de reconstruire un profil de la vie d'un individu - alors que la section 2(k) de la loi exclut le stockage d'informations liées à la race, la religion, la caste, la tribu, l'ethnicité, la langue, le revenu ou les antécédents médicaux dans le CIDR - le lien obligatoire d'Aadhaar avec divers programmes a permis le même résultat dans les faits [p. 907].

Le juge Chandrachud a également analysé la question de l'exclusion causée par les dispositifs biométriques ayant un impact disproportionné sur la vie des personnes marginalisées et des pauvres. Estimant que « le sort des individus ne peut être laissé aux vulnérabilités des algorithmes ou des dispositifs technologiques » [p. 930], il a également noté que l'exclusion arbitraire des avantages ou des subventions auxquels ils ont droit constitue une violation de la dignité. Selon lui, un tel refus de subventions et de prestations dû aux déficiences de la technologie biométrique est une menace pour la bonne gouvernance et la parité sociale [p. 932]. Au paragraphe 263, il remarque :

La question de l'exclusion doit être examinée à trois niveaux différents : (i) avant la mise en œuvre de la loi Aadhaar, lorsque les données biométriques étaient utilisées depuis 2009 ; (ii) en vertu des dispositions de la loi ; et (iii) au niveau pratique pendant la mise en œuvre du programme Aadhaar... Aucun taux d'échec dans la fourniture des prestations sociales ne peut être considéré comme acceptable. Les droits fondamentaux en matière de céréales alimentaires, par exemple, ne peuvent souffrir aucune erreur. Refuser de la nourriture, c'est conduire une famille à la misère, à la malnutrition et même à la mort.

Sur la question de la loi de finances et de la contestation d'une législation déguisée, l'opinion minoritaire a noté que le langage utilisé dans l'article 110(3) n'exclut pas le contrôle judiciaire de la décision du président, si la décision du président souffre d'illégalité ou d'une violation des dispositions constitutionnelles. En outre, il a souligné que pour être qualifié de loi de finances, un projet de loi doit

contenir « uniquement des dispositions » traitant de chacune ou de l'une des questions énoncées aux alinéas (a) à (g) de l'article 110(1). Par conséquent, un projet de loi tel qu'Aadhaar, dont certaines dispositions dépassent le champ d'application des alinéas (a) à (g) de l'article 110(1) et ne peuvent être supprimées, ne peut être considéré comme un projet de loi de finances. Étant donné que la loi Aadhaar crée un cadre légal pour l'obtention d'un numéro d'identité unique qui peut être utilisé à « n'importe quelle » fin, dont l'obtention d'avantages, de subventions et de services, pour lesquels des dépenses sont encourues à partir du Fonds consolidé de l'Inde, qui n'est qu'une des fins prévues par la section 7, elle ne répond pas à l'exigence de l'article 110(1). Par ailleurs, le juge Chandrachud a également souligné que même si l'on considère que l'article 7 a un lien avec les dépenses engagées à partir du Fonds consolidé de l'Inde, les autres dispositions de la loi ne relèvent pas du domaine de l'article 110(1).

Sur d'autres fronts, l'opinion minoritaire a également déclaré que les modifications apportées aux règles de 2005 relatives à la prévention du blanchiment d'argent (tenue de registres) ne répondaient pas au critère de proportionnalité, tandis que la section 139AA de la loi de 1962 relative à l'impôt sur le revenu était invalide car sa validité dépendait de la légalité de la loi Aadhaar, elle-même inconstitutionnelle. La décision de lier les numéros Aadhaar aux cartes SIM mobiles a également été déclarée inconstitutionnelle.

Opinion séparée mais concordante du juge Ashok Bhushan :

Selon l'opinion dissidente du juge Bhushan, l'obligation prévue par la loi Aadhaar de fournir des informations démographiques et biométriques ne viole pas le droit fondamental à la vie privée. En outre, les dispositions de la loi Aadhaar exigeant des informations démographiques et biométriques d'un résident pour l'obtention d'un numéro Aadhaar ont passé le triple test établi dans Puttaswamy I, et ne sont donc pas inconstitutionnelles. En outre, le juge Bhushan a noté que la collecte de données, leur stockage et leur utilisation ne violaient pas le droit à la vie privée.

L'opinion minoritaire était d'accord avec la Cour pour dire que le système ne créait pas une architecture pour une surveillance omniprésente, mais assurait au contraire la protection et la sécurité des données reçues des individus. En outre, il a également jugé les articles 7, 29, 33 et 47 de l'Aadhaar comme étant constitutionnelles, tandis que l'article 57 a été jugé inconstitutionnel dans la mesure où il permettait l'utilisation de l'Aadhaar par l'État ou toute personne morale ou physique, en vertu d'un contrat à cet effet. Il a également déclaré que la section 139AA de la loi sur l'impôt sur le revenu de 1961 et la règle 9 telle que modifiée par les règles PMLA (deuxième modification) de 2017 étaient constitutionnelles.

En outre, bien qu'il ne soit pas à l'abri d'un examen judiciaire, le juge Bhushan a estimé que la loi Aadhaar avait été adoptée à juste titre en tant que projet de loi monétaire. En ce qui concerne les

enfants, il a estimé que le consentement parental pour fournir des informations biométriques en vertu de la règle 3 et des informations démographiques en vertu de la règle 4 du Règlement Aadhaar (pour l'inscription et la mise à jour) de 2016 devait être lu pour l'inscription des enfants âgés de 5 à 18 ans pour confirmer la constitutionnalité de ces dispositions.

SENS DE LA DECISION

Issue : Restreint la liberté d'expression

L'arrêt de la Cour suprême de l'Inde restreint la liberté d'expression. L'évaluation de la majorité sur le caractère unique du système Aadhaar est discutable (comme le note le juge Chandrachud et en présence de preuves scientifiques du contraire). Sur la question de la protection des données et de la vie privée en particulier, si la Cour a correctement observé que l'adhésion aux principes de consentement, de limitation de la finalité et du stockage, de différenciation des données, d'exception des données, de minimisation des données, d'équité substantielle et procédurale et de garanties était nécessaire, elle a estimé que le système Aadhaar respectait ces principes (avec des exceptions concernant certaines dispositions de la loi qui ont été déclarées inconstitutionnelles). L'application des principes constitutionnels par la Cour dans cette affaire est cruciale pour établir le cadre de résolution des futurs litiges qui se situent à l'interface entre la technologie et les droits fondamentaux.

PERSPECTIVE GLOBALE

Sommaire des références

Normes, lois ou jurisprudences nationales

- Argentine, Constitution de l'Argentine (1853, rétablie en 1983), art. 19.
- Inde, Constitution de l'Inde (1949), art. 19.
- Inde, Constitution de l'Inde (1949), art. 21.
- Inde, Constitution de l'Inde (1949), art. 14.
- Inde, Chairman, All India Railway Recruitment Board c. K Shyam Kumar et autres (2010) 6 SCC 614.
- Inde, Ashoka Kumar Thakur (2008) 6 SCC 1
- Inde, Binoy Viswam c. Union of India et autres (2017) 7 SCC 59
- Inde, Kesavananda Bharati c. Union of India, 1973 Supp SCR 1
- Inde, People's Union of Civil Liberties (PUCL) et autres c. Union of India et autres, A.I.R. [2003] S.C. 2363.
- Inde, State of Bihar v. Project Uchcha Vidya, Civil Appeal No. 6626-6675 (2001).

- Inde, Ashoka Kumar Thakur (2008) 6 SCC 1
- Inde, Paschim Banga Ket Mazdoor Samity c. État du Bengale occidental (1996) 4 SCC 37
- Inde, Mohini Jain c. État du Kerala et Ors. (1992) 3 SCC 666
- Inde, Unnikrishnan c. État de l'Andhra Pradesh (1993) 1 SCC 645
- Inde, Olga Tellis c. Bombay Municipal Corporation (1985), 3 SCC 544.
- Inde, Justice Puttaswamy (Retd) & Anr c. Union of India & autres (2017), 10 SCC 1
- Inde, Subramanian Swamy c. Union of India, (2016) 7 SCC 221.
- Inde, Manoj Narula c. Union of India (2014), 9 SCC 1.
- Inde, Romesh Thappar c. État de Madras, (1950 SCR 594)
- Inde, State of Karnataka c. Shri Ranganatha Reddy (1977) 4 SCC 471.
- Inde, Dattatraya Govind Mahajan c. État du Maharashtra (1977) 2 SCC 548.

Lois internationales et/ou régionales pertinentes

- CJUE, Tele2 Sverige AB c. Postoch telestyrelsen, Secrétaire d'État au ministère de l'Intérieur c. Watson, affaires jointes C 203/15 et C 698/15 (2016).
- CJUE, Digital Rights Ireland Ltd c. ministre des communications, de la marine et des ressources naturelles, C 293/12 et C 594/12 (2014).
- CEDH, S. et Marper c. Royaume-Uni [GC], App. Nos. 30562/04 et 30566/04 (2008)
- CJUE, Affaire C 362/14, Maximillian Schrems c. Commissaire à la protection des données (2015)
- CEDH, Szabó et Vissy c. Hongrie, App. No. 37138/14 (2016)
- Afrique du Sud, S c. Jordanie et autres [2002] ZACC 22.
- États-Unis, Cruzan c. Directeur, Missouri Dept. de la Santé 497 US 361 (1990)
- États-Unis, Katz c. United States, 389 U.S. 347 (1967)
- États-Unis, Smith c. Maryland, 442 U.S. 735 (1979)
- Royaume-Uni, Wood c. Commissioner of Police for the Metropolis [2009] EWCA Civ 414.
- Afrique du Sud, Government of the Republic of South Africa et autres c. Grootboom et autres, 2001 (1) SA 46 (CC).
- CEDH, Budina c. Russie, App. No. 45603/05 (2009)
- États-Unis, Vernonia Sch. Dist. 47J c. Acton, 515 U.S. 646 (1995)
- Royaume-Uni, Murray c. Big Pictures U.K. Ltd [2008] EWCA 446.
- Canada, R. c. Oakes, [1986] 1 R.C.S. 103.
- Association québécoise des commissions scolaires protestantes c. Québec (P.G.) (1984) 2 SCR 66.

- Canada, R. c. Big M Drug Mart Ltd. (1985) 1 SCR 295
- Canada, Vriend c. Sa Majesté la Reine du chef de l'Alberta (1998), 1 SCR 493.
- Canada, R. c. Zundel, [1992] 2 R.C.S. 731.
- États-Unis, Lovell c. City of Griffin, 303 U.S. 444 (1938).
- États-Unis, Near c.. Minnesota, 283 U.S. 697 (1931)
- Royaume-Uni, Bidie c. General Accident, Fire and Life Assurance Corporation (1948) 2 All ER 995.
- États-Unis, Towne c. Eisner, 245 US 418
- Royaume-Uni, Jamesc. The Commonwealth [1936] UKPCHCA 4.

IMPORTANCE DE L'AFFAIRE

La décision établit un précédent contraignant ou persuasif dans sa juridiction. La décision (y compris les opinions concordantes ou dissidentes) établit un précédent influent ou persuasif en dehors de sa juridiction.

DOCUMENTS OFFICIELS DE L'AFFAIRE

- Jugement (anglais)