INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**



Vol. 7 - 2021

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

JUSTICE NUMÉRIQUE ET PROTECTION DES DONNÉES : UNE ÉTUDE COMPARATIVE ENTRE LA FRANCE ET LE BRÉSIL

par **Fernanda BRAGANÇA**, Doctorante en Sociologie et Droit à l'Universidade Federal Fluminense – Brésil. Chercheuse invitée à l'Université Paris 1 Panthéon-Sorbonne (2019-2020), Chercheuse associée au Centro de Inovação, Pesquisa e Administração do Judiciário – FGV, Avocate au Brésil.

La numérisation croissante de la justice et la récente législation sur la protection des données en France et au Brésil ont imposé une série d'adaptations du pouvoir judiciaire. Plus que jamais, le débat sur les postulats de transparence et de contrôle social des décisions judiciaires *versus* la protection de la vie privée a été relancé.

Malgré le fait que la France et le Brésil ont le même système juridique du *civil law*, les deux pays sont passés par des processus différents de divulgation de leurs décisions judiciaires.

La doctrine française propose une discussion approfondie qui intègre la disponibilité illimitée des décisions de justice sur l'internet avec la nécessité de protéger les données des parties au procès. Au Brésil, la profusion de l'intégralité des décisions sur l'internet dure depuis plus longtemps et cette question n'est que maintenant analysée à la lumière de la récente loi générale sur la protection des données personnelles.

Au Brésil, les décisions judiciaires déplacent un vrai *big data*. Selon le rapport *Justice en chiffres 2020*[1] publié par le Conseil national de la justice, le pouvoir judiciaire brésilien a enregistré 77,1 millions des affaires en attente d'une solution définitive. En 2019, plus des 20 millions de nouvelles actions ont été portées devant les tribunaux[2].

La structure judiciaire du pays est également assez complexe et comprend 91 tribunaux[3]: la Cour suprême fédérale, la Cour supérieure de justice (STJ), le Tribunal supérieur du travail (TST), la Cour électorale supérieure (TSE) et la Cour militaire supérieure (STM), les 27 tribunaux d'État (TJ), les cinq cours régionales fédérales (TRF), les 24 tribunaux régionaux du travail (TRT), les 27 tribunaux électoraux régionaux (TRE), les trois tribunaux militaires des États (TJM).

[1] Conselho Nacional de Justiça. *Justiça em números* 2020. Brasília: CNJ, 2020. Disponible à : https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justiça-em-Números-2020-atualizado-em-25-08-2020.pdf (consulté le 3 novembre 2020)

[2] Ibidem, p. 93.

[3] Ibidem, p. 9.

En ce sens, tout changement ou adaptation qui doit être apporté au système judiciaire brésilien doit être conçu pour une grande échelle. L'étude comparative est importante car elle permet la problématisation et l'amélioration des institutions.

§1 – MODÉLE D'ACCÈS OUVERT ET DE DONNÉS OUVERTES POUR LA DIFFUSION DES SOURCES DU DROIT

La publication de sources juridiques en général fait partie de la discussion sur l'accès aux données publiques. La disponibilité peut être faite par l'un des modèles suivants : l'accès ouvert ou les données ouvertes, qui sont universellement connus par les termes respectifs en anglais : *open access* et *open data*.

Dans le modèle du accès ouvert, les textes de législation et de jurisprudence sont publiés gratuitement et intégralement sur l'internet, mis à jour régulièrement et sont gratuits pour tous les types d'utilisation et de réutilisation. Le accès libre aux principales sources du droit est une condition essentielle du bon fonctionnement de l'État démocratique, dans la mesure où il garantit un contrôle a posteriori sur les décisions des magistrats par les citoyens.

Cependant, ce modèle n'est pas lisible par les machines et pour le traitement des informations, il faut d'abord le transformer en un format lisible par la machine, puis procéder au traitement lui-même. Seules quelques entreprises disposent des moyens financiers et techniques pour réaliser cette adaptation.

Dans le modèle des données ouvertes, les sources du droit sont librement accessibles au public et sont disponibles dans un format lisible par des machines et, par conséquent, traité par l'intelligence artificielle.

L'un des principaux avantages de ce modèle est qu'il permet la synchronisation automatique de ces changements législatifs, de sorte que la mise à jour commence instantanément. L'initiative des données ouvertes a connu son premier cadre juridique en Europe avec la directive 2003/98/UE[4] concernant la réutilisation des informations du secteur public.

En France, la disposition de la législation et de la jurisprudence choisie se font dans le modèle des données ouvertes. La législation peut être téléchargée au format RDF[5], facilement stockée en XML[6] et JSON[7], qui peuvent être facilement lues par n'importe quel langage de programmation.

Au Brésil, la législation ainsi que la jurisprudence brésilienne sont disponibles dans le modèle d'accès ouvert et le passage à un format de données ouvertes n'est pas encore à l'ordre du jour du

[4] Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, J.O. L 345 du 31/12/2003 pp. 0090 – 0096.
[5] Resource Description Framework.
[6] Extensible Markup Language.
[7] JavaScript Object Notation.

pouvoir judiciaire, bien que la numérisation soit l'un des objectifs fondamentaux pour les années à venir.

§ 2 – DIFFUSION DES DÉCISIONS DE JUSTICE EN FRANCE

La plupart des pays européens consacrent le principe de la publicité des procès. Même ainsi, seule une partie des États membres organise un régime standardisé pour la publication de ces décisions.

En France, toutes les décisions du Conseil constitutionnel et la plupart de celles rendues par la Cour de cassation depuis 1960 sont publiées. La base de données Légifrance contient plus de neuf cent mille dispositions en matière civile et pénale qui ont été sélectionnées par la cour d'appel et le tribunal de première instance. Cependant, le régime qui prévalait jusqu'à récemment est que la grande majorité de ces décisions étaient hors de accès gratuit au public.

L'initiative d'ouverture des données juridiques est inscrite en droit français depuis 1984, avec le décret n° 84-940[8], relatif au service public des bases de données et des bases de données et qui a créé le Centre national de l'informatique juridique (CNIJ), et avec le décret n° 96-481[9], relatif au service public des bases de données juridiques, qui comprenait les décisions des tribunaux administratifs et judiciaires. Cependant, les deux sont restés incomplets car les données ont été confiées à un revendeur et une partie importante de celles-ci n'est ouverte qu'avec un accès payant.

Les articles 20 et 21 de la loi pour une République numérique[10] sont donc le résultat d'un double mouvement : un plus général et

[8] Décret n°84-940 du 24 octobre 1984 relatif au service public des bases et banques de données juridiques. Disponible à :
https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006064639/1996-12-31/
(consulté le 3 novembre 2020)

[9] Décret n°96-481 du 31 mai 1996 relatif au service public des bases de données juridiques. Disponible à :
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000560581/2002-09-14/
(consulté le 3 novembre 2020)

[10] Article 20 – Modifie l'article L10 (M) du Code de justice administrative :
Art. L10 (M) – Les jugements sont publics. Ils mentionnent le nom des juges qui les ont rendus.
Ces jugements sont mis à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées.
Cette mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes.
Les articles L. 321-1 à L. 326-1 du code des relations entre le public et l'administration sont également applicables à la réutilisation des informations publiques figurant dans ces jugements.
Un décret en Conseil d'État fixe, pour les jugements de premier ressort, d'appel ou de cassation, les conditions d'application du présent article.
Art. 21 crée l'article L111-13 (M) du Code de l'organisation judiciaire :

> « Sans préjudice des dispositions particulières qui régissent l'accès aux décisions de justice et leur publicité, les décisions rendues par les juridictions judiciaires sont mises à la disposition du public à titre gratuit dans le respect de la vie privée des personnes concernées.

récent, avec une ouverture massive des données publiques, et une version plus ancienne et plus spécifique, pour la diffusion de la jurisprudence administrative et judiciaire.

La divulgation des décisions de justice entre pleinement dans le champ d'application du règlement général européen sur la protection des données, qui adapte les instruments de protection des données à caractère personnel de l'UE à l'évolution rapide des technologies[11].

Ces articles de la loi n° 2016-1321 impliquent directement la divulgation d'une quantité considérable de données personnelles, dont certaines présentent une sensibilité particulière et, de manière connexe, renforcent la protection des personnes concernées par les décisions par le respect de leur vie privée, conformément aux dispositions de la législation nationale et européenne sur ce sujet.

Néanmoins, les articles de de la loi pour une République numérique ne traitent pas sur la manière dont ce double garanti doit se matérialiser, se référant à la publication d'un décret par le Conseil d'État.

Le décret n° 2020-797 du 29 juin 2020[12] prévoit la mise à disposition publique des décisions des juridictions judiciaires et administratives. Le décret institue le Conseil d'État comme chargé de rendre les décisions administratives accessibles au public sous forme électronique. De même, la Cour de cassation est responsable de la mise à la disposition au public, sous forme électronique, des décisions de justice rendues par les juridictions judiciaires.

Toutes les décisions seront publiées sur un portail internet sous la responsabilité du garde des sceaux ministre de la justice. Ce site *Web* devrait indiquer les contacts et la manière dont les parties intéressées peuvent faire valoir leurs droits d'accès, de rectification et d'occultation des informations personnelles, conformément au règlement européen sur la protection des données.

Le décret prévoit également que l'occultation des noms des parties ou des tiers sera effectuée systématiquement. Si, même

---

> Cette mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes.
>
> Les articles L. 321-1 à L. 326-1 du code des relations entre le public et l'administration sont également applicables à la réutilisation des informations publiques figurant dans ces décisions.
>
> Un décret en Conseil d'État fixe, pour les décisions de premier ressort, d'appel ou de cassation, les conditions d'application du présent article. »

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Disponible à : https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/ (consulté le 5 novembre 2020)

[11] Ibid., p. 20.

[12] Articles 1 et 4

Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives. Disponible à https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042055251/ (consulté le 5 novembre 2020)

avec cette désidentification, la décision atteinte à la sécurité ou au respect de la vie privée des personnes physiques mentionnées au jugement ou de leur entourage, le juge qui a rendu la décision ou le président de la formation du jugement peuvent décider sur l'occultation d'autres élément.
L'occultation du nom des magistrats est également prévue dans ce décret. Dans le cadre de la juridiction administrative, cette décision est prise par le président de la section du contentieux du Conseil d'État, le président de la cour administrative d'appel ou le président du tribunal administratif. Au sein de la juridiction judiciaire, cette question est décidée par le président du tribunal concerné.
Les premières décisions diffusées en *open data* seront les arrêts de la Cour de cassation en septembre 2021. Depuis, les décisions civiles, sociales et commerciales des cours d'appel à la fin du premier semestre 2022[13].
Dans la juridiction judiciaire, les dates de diffusions des décisions seront fixées après la levée des conditions techniques de mise en œuvre des concessions prévues par la loi sur le portail « Portalis » en matière civile et « procédure pénale numérique » en matière pénale[14].

Problématisation de la diffusion des données décisionnelles en France

Les règles de protection de la vie privée du citoyen prévoient que les décisions de la justice sont diffusées au regard de la vie privée et que cette mise à la disposition du public doit être précédée d'une analyse du risque de réidentification des personnes.
Le législateur français, en évoquant le « respect de la vie privée », a opté pour une connotation nettement différente de « protection des données personnelles », même si les deux expressions ont de nombreuses corrélations entre elles. La protection des données personnelles est comprise comme un élément de la vie privée, mais elle n'est pas complètement couverte par cette notion, car certaines informations peuvent ne pas être liées à la vie privée de l'individu[15].
Les débats législatifs dans le cadre de la commission mixte (CMP) ont montré qu'il ne suffit pas d'occulter l'identité des personnes dans les décisions pour protéger leur vie. Au contraire, les parlementaires sont très prudents sur la question de la ré-identification et confient à l'autorité de régulation la tâche de

[13] Cf. A. DUMOURIER, « Open data des décisions de justice : publication du décret au JO », *Le Monde du droit,* 1 juillet 2020. Disponible à: https://www.lemondedudroit.fr/decryptages/70600-open-data-decisions-justice-publication-decret-jo.html (consulté le 5 novembre 2020)
[14] Ibidem.
[15] L. CADIET, *L'open data de décisions de Justice*, Mission d'étude et de préfiguration sur l'overture au public des décisions de justice, Rapport à madame la garde des sceaux, ministre de la justice, 2017, p. 34.

déterminer les conditions qui doivent être présentes afin d'assurer un équilibre entre la diffusion de l'information et la prévention des risques avec la même[16].

Les notions d'« anonymisation » et de « pseudonymisation » sont issues des dispositions du droit européen et du droit national français. L'article 4, (5)[17] et le considérant n° 26[18] du règlement (UE) 2016/679 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 définissent que la « pseudonymisation » constitue un traitement de données à caractère personnel qui est effectué de telle manière qu'il ne peut plus être attribué à une personne concernée spécifique sans l'utilisation d'informations supplémentaires; qui sont gérées séparément et soumises à des mesures techniques et organisationnelles pour garantir que les données ne sont pas attribuées à une personne physique identifiée ou identifiable. La mise en œuvre de la « pseudonymisation » complique donc l'identification des sujets, mais n'a pas pour effet de l'empêcher totalement. Ainsi, l'individu reste identifiable.

La notion de « anonymisation » peut être déduite de informations anonymes[19] définis comme ceux qui n'ont aucun lien avec une personne identifiée ou identifiable. Ainsi, l'anonymat suppose donc qu'il n'y ait plus de lien possible entre les données et la

---

[16] Ibidem.

[17] Article 4 (5):

> « "pseudonymisation", le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable; »

[18] Considérant n° 26:

> « Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »

[19] Considérant (26) du règlement (UE) 2016/679.

personne à laquelle elles se rapportent. De cette manière, l'identification devient alors totalement impossible.

Les décisions actuellement rendues publiques, notamment via le portail Légifrance, sont pseudonymisées, basée sur la résolution CNIL n° 01-057 du 29 novembre 2001[20], qui recommande la suppression des noms et adresses des parties et témoins du procès. La protection établie n'empêche donc pas toute identification ultérieure des personnes impliquées.

À l'époque, la possibilité de diffuser ces décisions judiciaires impliquant des données personnelles reconnues par la résolution précitée reposait sur un équilibre entre l'intérêt légitime de l'utilité documentaire de la diffusion de la jurisprudence et la protection de la vie privée des citoyens.[21] Cependant, à ce moment, ce cadre est devenu insuffisant. Il semble désormais nécessaire de le revoir à la lumière des événements suivants : nouveau contexte technologique ; la divulgation d'une quantité disproportionnée de données par rapport à ce qui est actuellement publié en ligne; et mise à jour du système juridique, notamment au niveau européen sur ce sujet.

Dans un premier temps, ce nouveau scénario pourrait indiquer que la solution serait l'option d'anonymiser les décisions de la justice. Pourtant, l'analyse des dispositions légales applicables et l'état de la technique rendent cet objectif extrêmement complexe, voire impossible à atteindre.

L'anonymat d'une décision de justice présuppose que les personnes ne sont plus identifiées directement ou indirectement, par un processus de désidentification irréversible et prend en compte l'état actuel de la technologie, mais surtout les perspectives futures d'évolution des ressources technologiques. Pour le moment, la réponse à ces attentes n'est pas viable.

La simple suppression des informations personnelles des décisions est insuffisante pour répondre aux exigences

---

[20] Cette délibération reconnaissait que

> « Le souci du juste équilibre ne saurait conduire à préconiser d'ôter tout caractère indirectement nominatif, au sens de l'article 4 de la loi du 6 janvier 1978, aux décisions de justice. Une telle orientation serait tout à fait disproportionnée, susceptible de nuire à la lecture de la décision ou contraindrait dans bien des cas à ne pas diffuser telle ou telle décision au motif que sa lecture seule permettrait d'identifier les parties en cause. Elle serait, par nature, contraire à la finalité légitime poursuivie par les juridictions ou les éditeurs de jurisprudence consistant à offrir un outil documentaire le plus complet et le plus accessible possible. Ce même souci de l'équilibre ne serait pas atteint si le nom et l'adresse des personnes ayant été, d'initiative ou malgré elles, parties à un procès, continuaient à figurer sur les décisions de justice librement accessibles sur Internet, le plus souvent d'ailleurs sans qu'elles en aient conscience et sans qu'elles en pèsent les incidences. »

CNIL, délibération n ° 01-057 du 29 novembre 2001, portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence. Disponible à:
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000017653503/ (consulte le 13 novembre 2020)

[21] L. CADIET, *L'open data de décisions de Justice*, Mission d'étude et de préfiguration sur l'overture au public des décisions de justice, op. cit., p. 35.

d'anonymat car les décisions de la justice contiennent une très grande quantité d'informations qui permettent une ré-identification des parties, notamment dans le raisonnement juridique, qui contient plusieurs éléments contextuels qui peuvent conduire à des références croisées avec d'autres bases de données[22].

Ainsi, selon le rapport du professeur Loic Cadiet, la « pseudonymisation » des décisions de justice apparaît actuellement comme la seule option techniquement réalisable dans le contexte de la divulgation publique, cadre normatif imposé par les articles 20 et 21 de la loi pour une République numérique et le RGPD[23].

En ce sens, la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice a déclaré dans sa recommandation n°. 5 que le décret du Conseil d'État devrait prévoir la mise en œuvre de la « pseudonymisation » à l'égard de toutes les personnes physiques mentionnées dans les décisions des tribunaux, sans le limiter aux parties et aux témoins dans le processus (avec la sauvegarde des noms des professionnels du droit, dont la situation n'a pas encore été analysée).

Il convient également de mentionner que le cadre juridique de la protection des données personnelles ne se limite pas à leur diffusion, mais il s'étend aussi à sa réutilisation par ceux qui y ont eu l'accès[24]. Cependant, ce n'était pas la ligne suivie par le décret du Conseil d'État qui visait à assurer la diffusion immédiate au public des décisions de justice.

§ 3 – PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

La pandémie de Covid-19 a intensifié les cyberattaques et diversifié les menaces à la sécurité informatique. L'accélération de la digitalisation des différentes tâches humaines contribue à la croissance de ce phénomène qui nécessite la formulation de stratégies renouvelées par le pouvoir public, qui comprend l'institution judiciaire. Ce nouveau volume de données sur le réseau résultant de la migration massive et instantanée de diverses activités vers le cyberespace a provoqué une véritable rupture au niveau juridique, social et organisationnel[25].

La cybercriminalité est un sujet qui a fait l'objet de débats intenses au sein de l'Union européenne et dans les États membres, car ce type d'attaque contre des entreprises et institutions publiques permet le chantage et l'obtention de sommes importantes par des criminels.

---

[22] Ibidem, p. 36.
[23] Ibidem.
[24] Ibid., p. 37.
[25] M. QUÉMÉNER. « Virus et pandémie numériques: actualités en matière de cyberattaques », *Revue Pratique de la Prospective et de l'innovation*, nº 2, octobre 2020, p. 19.

A) La sensibilisation à la sécurité des données en France

L'agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le « Guide pour sensibiliser les entreprises et les collectivités »[26] avec quelques suggestions de mesures de sécurité ou d'hygiène informatique afin de décrocher qu'un rançongiciel n'atteigne l'organisation ou de réduire les pertes.

Les principaux conseils proposés par l'ANSSI sont : utilisation et mise à jour de logiciels antivirus[27], cloisonnement du système d'information[28], limitation des droits des utilisateurs et autorisations des applications[29], évaluation de l'opportunité d'inscription à une assurance cyber[30], définition d'une stratégie de communication cyber[31], plan de réponde aux cyberattaques[32] et sensibilisation des collaborateurs[33].

L'utilisation et mise à jour d'logiciels antivirus ne garantissent pas de protéger l'entité de rançongiciels encore inconnus mais peuvent, dans la majorité des cas, empêcher une compromission et éviter le chiffrement des fichiers. Toutefois, pour que ces outils soient efficaces, il est important d'effectuer une mise à jour fréquente des signatures et de s'assurer régulièrement de l'absence de logiciel malveillant connu sur les espaces de stockage des fichiers de l'institution.

Le cloisonnement du système d'information a pour but la limitation du risque de propagation du virus. Il convient de mettre en place un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système. Un cloisonnement des niveaux d'administration peut également être mis en place afin de s'assurer que les niveaux les plus hauts soient difficilement atteignables par les attaquants.

Un exemple de bonne pratique de sécurité est la limitation des droits des utilisateurs et autorisations des applications. Cette pratique consiste que les utilisateurs ne sont pas administrateurs de leur système de travail. Ainsi, l'installation de logiciels et l'exécution involontaire de codes malveillants seront impossibles par défaut. Par contre, les actions de propagation du rançongiciel au sein du système d'information sont généralement réalisées à l'aide de comptes d'administration, notamment lors des attaques de type « *Big Game Hunting* ». Il est donc nécessaire de limiter le

[26] Cf. ANSSI. *Guide pour sensibiliser les entreprises et les collectivités*, 4 septembre 2020. Disponible à : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf (consulté le 9 novembre 2020)
[27] Ibidem, p. 12.
[28] Ibidem, p. 13.
[29] Ibidem, p. 14.
[30] Ibidem, p. 18.
[31] Ibidem, pp. 21-22.
[32] Ibidem, pp. 19-20.
[33] Ibidem, p. 17.

nombre de ces comptes au strict nécessaire et de porter une attention particulière à l'utilisation qui en est faite.
La définition d'une stratégie de communication cyber est essentielle pour diminuer les impacts de la crise sur l'image et la réputation de l'institution, tant en interne qu'en externe. Un plan de réponse aux cyberattaques associé au dispositif de gestion de crise sont indispensables pour assurer la continuité d'activité puis son retour à un état nominal. La mise en œuvre d'un plan de continuité informatique doit permettre à l'organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information.
La sensibilisation des collaborateurs est une explication fondamentale : une grande partie des attaques par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape primordiale pour lutter contre cette menace.
Les différends documents[34] qui traitent de ce sujet avertissent sur l'impréparations des institutions privées et publiques face aux cyberattaques. Selon une enquête menée par la société internationale de cyber sécurité Kaspersky[35], près de la moitié (46,69%) des 1,3 million de tentatives d'attaques par *ransomware*[36] en Amérique latine entre janvier et septembre 2020 concernent le Brésil.
Compte tenu de ce scénario, il est très important que toutes les institutions brésiliennes, y compris le pouvoir judiciaire, soient préparées avec systèmes de cyber sécurité mises à jour afin qu'une éventuelle attaque ne provoque pas de violation ou suppression d'informations ou de dommages aux parties du procès.

B) Le système judiciaire et la protection des données au Brésil

Au Brésil, dès 2007, l'intégralité des décisions de Justice sont publiées dans le cyberespace et les juges n'ont jamais procédé à aucune sélection pour cette diffusion. La consultation des décisions peut se faire via les sites Web des tribunaux à travers le numéro de dossier, le nom de la partie ou de l'avocat par tout

[34] Cf. J. BASCHER, *La sécurité informatique des pouvoirs publics : rapport d'info nº. 82 (2019-2020)*, 22 octobre 2019, fait au nom de la comission des finances. Disponible à: https://www.senat.fr/rap/r19-082/r19-0821.pdf (consulté le 9 novembre 2020)
[35] Cf. A. ROSA et al., « Brasil conta com poucas armas legais para combater ataques de hackers », *Jornal Valor Econômico*, legislação e tributos, 7-9 novembre 2020.
[36] "Ransomware est un logiciel informatique malveillant, bloquant les données qui chiffre les fichiers contenus sur les ordinateurs et demande une rançon en échange d'une clé permettant de les déchiffrer. Le ransomware s'infiltre sous la forme d'un ver informatique, à traver um fichier de la victime. La finalité est d'extorquer une somme d'argent à payer le plus souvent par monnaie virtuelle pour éviter toute trace.", M. QUÉMÉNER, « Virus et pandémie numériques : actualités en matière de cyberattaques », op. cit., p. 19.

citoyen, à l'exception des procédures qui sont protégés par le secret de justice.

La protection des données personnelles a gagné en pertinence avec la promulgation d'une loi spécifique à ce sujet en 2018. La législation a été inspirée par le règlement européen et a pour objectif principal la plus grande transparence et simplicité dans le contrôle du traitement des données par les citoyens.

La loi nº 13.709/2018 prévoit dans son chapitre IV des règles pour le gouvernement. L'article 23 établit que le traitement des données à caractère personnel par des personnes de droit public doit être effectué pour remplir leur finalité publique, dans la poursuite de l'intérêt public, dans le but d'exécuter les pouvoirs juridiques ou pour accomplir les attributions de la fonction publique.

Le contenu normatif est assez générique et ne mentionne pas expressément son application aux services de justice. La disposition se réfère cependant aux entités énumérées à l'article 1 de la loi nº 12 527/2011 sur l'accès à l'information, qui inclut le pouvoir judiciaire. Par conséquent, la norme indique indirectement que les tribunaux devront se soumettre au LGPD.

Le législateur européen, pour sa part, a été plus objectif en déclarant que le règlement sur la protection des données est également applicable aux activités des tribunaux et autres autorités judiciaires. L'Union et les États membres peuvent légiférer sur ce sujet pour déterminer les opérations et les procédures auxquelles il s'applique. La législation précise, cependant, qu'elle ne concerne pas le traitement des données à caractère personnel effectué dans l'exercice de sa fonction juridictionnelle (considérant n° 20 du RGPD).

Malgré cette nouvelle législation, la discussion sur l'ouverture de l'information et la diffusion des décisions est très peu débattue car cette disponibilité s'est déjà produite dans son intégralité et avec toutes les informations contenues dans les actes de procédure.

Le Conseil national de la justice a publié la recommandation n° 73/2020[37], avec la proposition d'établir un plan national de protection des informations personnelles existant dans les bases de données des tribunaux[38].

La recommandation prévoit l'élaboration d'un plan d'action, la publication de la politique de confidentialité sur les sites électroniques ainsi que des enregistrements relatifs au traitement des données personnelles par les tribunaux et la mise en place

[37] Conselho Nacional de Justiça. Recomendação nº 73 de 20/08/2020. Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD. Disponible à : https://atos.cnj.jus.br/atos/detalhar/3432 (consulté le 11 novembre 2020)

[38] Cf. Cumprimento da LGPD. «Recomendação do CNJ orienta tribunais sobre proteção de dados». *Revista Consultor Jurídico*, 27 de agosto de 2020. Disponible à : https://www.conjur.com.br/2020-ago-27/recomendacao-cnj-orienta-tribunais-protecao-dados (consulté le 11 novembre 2020)

d'un groupe de travail dans chaque Cour pour étudier et identifier les mesures nécessaires à la mise en œuvre de la LGPD.

Le CNJ a créé un groupe de travail.[39] visant à analyser les ajustements nécessaires à la mise en œuvre de la LGPD au sein du pouvoir judiciaire. C'est à partir de cette étude que le Conseil formulera un règlement national pour la protection des données personnels devant les tribunaux. Tous les portails institutionnels doivent expliquer leur politique de confidentialité à leurs utilisateurs.

Le CNJ est mobilisé pour adapter le pouvoir judiciaire au nouveau contexte de la protection des données et le conseiller Rubens Canuto, lors de la 71e séance plénière, a souligné dans sa décision[40] l'importance que le Conseil agisse en coopération avec l'autorité nationale de protection des données afin d'assurer le bon respect de la législation sur ce sujet dans tous les tribunaux du pays[41].

Récemment, la Cour supérieure de justice [42] a enregistré une cyberattaque dans son système. Le criminel a temporairement bloqué l'accès à la base de données du STJ avec l'utilisation du cryptage, mais ils sont restés conservés dans les systèmes de sauvegarde du tribunal.

L'attaque a inquiété le pouvoir judiciaire. Le risque de fuite d'informations découlant d'affaires protégées par le secret de justice et la nécessité d'arrêter les activités de la Cour sont les points qui ont le plus retenu l'attention des autorités.

La digitalisation croissante des tribunaux[43] a également contribué à l'augmentation du niveau d'alerte du pouvoir judiciaire à mesure qu'une grande quantité des données sont allouées dans le système *cloud*.

En cas de violation de contenu confidentiel personnel ou d'exposition de données sensibles d'entreprises à la suite de cet acte de piratage, le STJ peut être tenu pour responsable au titre de la loi générale sur la protection des données, s'il est prouvé que le

---

[39] Conselho Nacional de Justiça. Portaria, n° 63 de 26/04/2019. Institui Grupo de Trabalho destinado à elaboração de estudos e propostas voltadas à política de acesso às bases de dados processuais dos tribunais e dá outras providências. Disponible à : https://atos.cnj.jus.br/atos/detalhar/2890 (consulté le 11 novembre 2020)

[40] Ibidem.

[41] Cf. F. BRAGANÇA; F. G. MIRANDA NETTO. « Proteção de dados e Poder Judiciário: reflexões a partir da LGPD e da experiência espanhola », *Anais do IV Seminário Internacional de Direitos Humanos Fundamentais*, Vol. 1, Direitos Fundamentais de Primeira Dimensão: Direitos Civis & Políticos, 2020, Zoom et Google Meet, pp. 233-246.

[42] Par la *Portaria STJ / GDG* no. 590 du 18 septembre 2020 (Brésil), la Cour a institué une commission dans le but de préparer une étude et d'identifier les mesures nécessaires à la mise en œuvre de la LGPD dans le STJ. Les travaux de la commission sont déjà en cours. Disponible à : https://bdjur.stj.jus.br/jspui/handle/2011/147139 (consulté le 11 novembre 2020)

[43] La résolution CNJ 185/2013 (Brésil), qui a institué le système de processus judiciaire électronique (PJe) en tant que système de traitement de l'information et la pratique des actes de procédure, a eu un impact significatif sur le pourcentage d'affaires déposées électroniquement, qui est passé de 30,4% en 2013 à 90 % en 2019 (CNJ, 2020, p. 258).

pouvoir judiciaire n'a pas utilisé les formes de sécurité propres[44]. Certains juristes soutiennent que la réparation du préjudice causé au titulaire par les institutions publiques ne dépend pas du dommage matériel et même de la survenance effective d'une fuite de données. Cependant, c'est une question qui est encore sans précédent et le pouvoir judiciaire lui-même jugera une éventuelle action de réparation des dommages.

Tandis que l'autorité nationale brésilienne de protection des données et le CNJ ne publient pas de lignes directrices plus concrètes sur la protection des données et la cybersécurité, l'expérience étrangère, notamment européenne, peut contribuer à la lutte contre les attaques numériques au Brésil. Sans doute, les efforts impliquent la coopération des organisations nationales publics et privés et internationales.

[44] L. IGNACIO; J. BACELO, "LGPD pode ser usada contra o STJ", *Jornal Valor Econômico, legislação e tributos*, 7-9 novembre 2020.