RAPPORT GÉNÉRAL

LE DROIT PUBLIC
ET LES NOUVELLES TECHNOLOGIES INFORMATIQUES

2019

AIHJA
IASAJ
Association Internationale
des Hautes Juridictions Administratives

SOMMAIRE

1 /// RAPPORT GENERAL

2 /// COMPTE-RENDU DES TRAVAUX EN COMMISSION

3 /// QUESTIONNAIRE

RAPPORT GENERAL

/// SUJET 1

IMPACT DES TECHNOLOGIES NUMERIQUES SUR LES JURIDICTIONS ADMINISTRATIVES

1.1] Environnement numérique en matière administrative

Question n°1 :

L'identification électronique. Existe-t-il un registre des fonctionnaires publics et des représentants légaux dans la législation nationale ? Dans l'affirmative, comment est-il réglementé ? Quelle est sa nature ?

L'existence de registres des fonctionnaires et des représentants légaux dans la législation nationale est un aspect important de la transparence de l'administration publique de n'importe quel Etat, puisque ces registres permettent aux administrés de connaître le nombre d'agents publics, leurs profils et leurs fonctions, afin d'avoir la certitude de l'identité des agents publics qui ordonnent et exécutent un acte administratif, ainsi que des professionnels autorisés conformément aux lois à assurer la représentation du particulier auprès des entités publiques.

Parmi les Etats faisant partie de l'**Association Internationale des Hautes Juridictions Administratives**, nous remarquons que la Colombie, la Suisse, la Finlande, l'Italie et le Mexique disposent de registres nationaux des agents publics et d'un registre public des professionnels.

À titre d'exemple, l'Annuaire Fédéral Suisse est disponible en ligne et accessible au public. Il contient les noms des membres de l'Assemblée Fédérale (Parlement Suisse), des membres des tribunaux fédéraux (juges et greffiers), des membres du Conseil Fédéral et du Chancelier de la Confédération Helvétique. De même, y apparaissent les noms, fonctions et coordonnées des personnes exerçant de hautes fonctions dans l'Administration Fédérale, les Services Parlementaires et les autres principales organisations de droit public chargées de missions en lien avec l'action publique de la Confédération.

La Suisse dispose également d'un registre public des représentants légaux contenant des informations que chaque membre de l'Assemblée Fédérale doit déclarer lors de sa prise de fonctions et au début de chaque année calendaire. Les informations à déclarer sont les suivantes :

Ses activités professionnelles : s'il est employé, le membre doit spécifier sa position et son employeur ;

- Toute fonction de gestion, supervision, conseil ou autres occupée au sein d'organismes, entreprises, institutions ou fondations suisses ou étrangères, de droit privé ou de droit public ;
- Les missions de conseil ou d'expertise réalisées au nom de la Confédération ;
- Les missions permanentes de gestion ou de conseil réalisées au nom de groupes d'intérêts suisses ou étrangers ;

❊ Les fonctions occupées dans les comités ou autres organes de la Confédération.

En Grèce et au Bénin, il existe un registre des fonctionnaires publics. Pour la Grèce, il s'agit d'un registre électronique des ressources humaines qui liste, entre autres, tous les membres du pouvoir judiciaire, le personnel des tribunaux et les agents du Conseil Juridique de l'Etat. Concernant le Bénin, le ministère du Travail et de la Fonction Publique tient un fichier numérique recensant des informations sur ses employés et leur performance.

Le Canada, lui aussi, dispose d'une liste d'agents publics fédéraux, ainsi que de leurs bureaux, intégrée dans le Répertoire en ligne du Gouvernement canadien. Les avocats sont recensés dans des répertoires publiés par des éditeurs privés plutôt que dans un registre tenu par l'administration.

La Norvège, quant à elle, ne dispose pas d'un registre central de ses fonctionnaires, mais chaque administration ou institution tient une liste de ses fonctionnaires. C'est aussi le cas de l'Autriche, la Chine et la France.

Il en est de même pour l'Allemagne, la République Tchèque, les Pays-Bas, la Hongrie, la Pologne et le Portugal, qui utilisent comme Registre national de représentants, les listes dont disposent leurs Barreaux respectifs.

Une situation particulière est celle de la Turquie, où, pour pouvoir être enregistrés à la Commission de Justice turque et donc accéder aux droits que confère ledit registre, les professionnels doivent être affiliés à l'Union des Barreaux Associés de Turquie.

Parmi les Etats membres de l'Association, certains ne disposent pas de registre. Nous pouvons citer la Belgique, le Luxembourg, la Corée du Sud, la Slovaquie et la Lituanie, tandis que la Thaïlande possède un registre de la population générale, conformément à sa Loi d'Enregistrement et d'Identification, mais pas de registres des agents publics ou de représentants.

Question n°2 :

Transparence et accès à l'information. Quelles sont les obligations des juridictions, en particulier administratives, en matière de diffusion de vos données et sentences (open data) ?

Lorsqu'ils saisissent les juridictions administratives, les particuliers attendent de celles-ci qu'elles rendent des décisions sur les actes des autorités administratives qu'ils considèrent illégaux ou arbitraires. Par conséquent, le fait de rendre publiques les décisions des juridictions, garantit l'impartialité, la transparence et l'assujettissement aux règles du procès équitable.

Une partie des Etats membres de l'AIHJA diffuse, après anonymisation, des versions publiques de leurs décisions, lesquelles sont diffusées via leurs sites web. Les parties sont destinataires d'une version non anonymisée. C'est le cas dans les pays suivants : Autriche, Bénin, Suisse, Israël, Corée, Slovaquie, Finlande, France, Grèce, Pologne, Portugal, Lituanie et Mexique, où les versions publiques omettent les données rendant possible l'identification des parties ou des tiers.

En général, les législations des Etats mentionnés entendant par « données rendant possible l'identification des parties » les prénoms et noms de famille des personnes physiques mentionnées dans la décision quand il s'agit de parties ou de tiers, ainsi que tout élément permettant d'identifier les parties et les tiers et toute information que les diverses législations peuvent considérer comme réservée ou confidentielle. Ces informations sont omises dans la version publique.

En Allemagne, aux Pays-Bas, au Luxembourg et en Turquie, bien qu'il n'y ait pas de dispositions spécifiques sur l'anonymat et la présentation des données, la pratique des tribunaux est d'appliquer cet anonymat pour les données personnelles dans les décisions diffusées par voie électronique.

D'autres pays publient leurs décisions avec un certain degré d'anonymat incluant, pour certains cas particuliers, l'omission de données sensibles. Il s'agit de la Chine, du Canada, de l'Australie, de l'Espagne, de la Hongrie, de la Norvège et de la Belgique, où il est commun que soient omis certains renseignements dans des cas où des mineurs se trouvent impliqués et pour certaines victimes de crimes. La République Tchèque, en général, publie ses décisions en rendant anonymes les noms et les données sensibles des parties, excepté dans les cas de protection internationale où les décisions ne sont pas publiées.

Pour sa part, la Colombie transmet de façon ouverte ses données, via le site web du Conseil d'Etat, notifiant les décisions aux organismes publics par courrier spécifiquement créé à cet effet. En matière civile, les données sont également diffusées électroniquement sans anonymat.

Finalement, il existe des juridictions, comme en Côte d'Ivoire qui, s'agissant de la Chambre Administrative, ne diffusent pas de données ou de décisions. La Cour Suprême du Sénégal, quant à elle, publie les décisions d'intérêt particulier sur son portail Internet. En principe, la publication est décidée par les juges à la fin de leurs délibérations. Ainsi, les Présidents de chambres transmettent chaque année au Service de la Documentation et des Etudes de la Cour, les jugements sélectionnés et leurs résumés pour publication.

Question n°3 :

La démocratie informatique. Votre pays recourt-t-il aux outils informatiques pour l'expression de la volonté populaire (élections, consultations du public, etc.) ? Dans l'affirmative, comment est assurée la sécurité des consultations ?

Pour ce qui a trait à l'utilisation d'outils numériques pour l'exercice du vote, il existe, parmi les pays membres de l'Association Internationale des Hautes Juridictions, des Etats ayant mis en place des procédures de suffrage numérique pour les processus électoraux, d'autres ont recours à ces dispositifs pour les référendums et d'autres continuent d'avoir recours aux bulletins de vote traditionnels.

La Pologne, le Portugal et la Suisse utilisent des systèmes de vote électronique pour les élections locales. Depuis les élections de mars 1973, la France utilise également, dans certaines communes, des machines de vote électronique. Récemment, le Mexique a autorisé ses citoyens résidants à l'étranger à voter de manière électronique.

Il existe des Etats ayant recours à un système mixte. Tel est le cas de la Belgique où la loi du 7 février 2014 permet d'émettre le suffrage par voie électronique mais complété d'un support papier.

L'Allemagne, l'Autriche, la Grèce, la Hongrie, le Luxembourg, la Slovaquie, la Thaïlande et la Turquie n'ont pas recours au vote électronique pour l'élection de leurs représentants, bien qu'ils le fassent pour présenter des propositions aux parlements et réaliser des consultations publiques, alors que la Corée du Sud le permet pour l'élection des membres de certaines institutions et entités approuvées par la Commission Nationale Electorale.

La Colombie ne dispose pas d'un tel système de vote électronique mais a adopté une loi permettant qu'un tel système soit mis en place.

D'autres Etats, comme la Finlande et les Pays-Bas, ont tenté de mettre en place un système de vote électronique mais, en raison de circonstances particulières, ont décidé de reporter l'utilisation de ce mécanisme, revenant pour le moment au suffrage sur papier.

Au sein du groupe d'Etats qui ne prévoient pas le recours au vote électronique et préfèrent les bulletins papier, se trouvent le Bénin, la République Tchèque, la Côte d'Ivoire, la Norvège, l'Italie, le Canada, la Lituanie, le Sénégal et la Suède.

1.2] Outils informatiques et travail du juge

Question n°1 :

Aspects inhérents au télétravail. Les juges administratifs ont-ils la possibilité de travailler à distance ? Dans l'affirmative, quels sont les outils informatiques et électroniques mis à leur disposition (application spécifique, portail en ligne, VPN, …) pour traiter les dossiers à distance ?

Grâce à l'utilisation de nouvelles technologies et des progrès dans leur sécurité, il existe désormais la possibilité de travailler à distance de manière sûre et fiable. Ceci est utile en particulier pour éviter des pertes de temps dans les transports ou en situations d'urgence - comme cela a été le cas au Mexique lors du séisme de septembre 2017. Cela permet d'assurer les tâches depuis le domicile lorsque l'agent se trouve hors de sa zone de travail.

Normalement, les plateformes numériques utilisées par les organismes juridictionnels sont accessibles via un Wi-Fi, sans besoin d'une connexion physique au réseau des tribunaux, puisque les sites sont disponibles sur Internet et accessibles par tous les usagers avec un code d'accès et un mot de passe, voire, dans certains cas, grâce à un système en deux étapes de double vérification de la signature électronique, d'abord par un mot de passe renforcé et ensuite un message de confirmation. En ce qui concerne les juges, ceux-ci peuvent accéder aux dossiers électroniques depuis leur domicile par le biais de leur ordinateur professionnel ou personnel, utilisable comme bureau virtuel, à condition que leur matériel informatique soit correctement enregistré sur le domaine, leur permettant de consulter le dossier et les documents numériques qui y sont contenus, de rechercher la jurisprudence, de suivre et prendre les actes de procédures, y compris d'émettre leur décision définitive. Parmi les pays disposant d'un tel système se trouvent l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Chili, la France, la Finlande, la Grèce, les Pays-Bas, le Portugal, le Mexique, la Norvège, l'Italie, Israël et la Turquie.

En Espagne, la seule juridiction ayant entièrement numérisé sa procédure est l'Audience Nationale, où les juges disposent de tous les outils pour le télétravail, y compris un portail en ligne avec des archives numérisées, un VPN et une signature électronique.

Pour ce qui est de la République Tchèque et de la Suède, les juges peuvent travailler à distance sur leurs bases de données à travers un Réseau Privé Virtuel (VPN) de façon sûre. Au Luxembourg, ce système n'est pas interdit, cependant les juridictions ne disposent pas d'une plateforme spéciale pour ce faire.

De leur côté, les juridictions administratives polonaises auront, à partir de mai 2019, un accès à distance aux archives judiciaires ainsi qu'au documents électroniques présentés par les parties dans les procédures.

La Thaïlande projette de mettre en œuvre le système E-ADMINCOURT qui sera disponible au public et permettra au juge de travailler à distance, de consulter la jurisprudence et les bases de données. Il en est de même pour la Slovaquie où la juridiction électronique et l'établissement du classement légal électronique sont en phase de développement. Pendant ce temps, les deux juridictions travaillent déjà à distance avec une connexion VPN.

Finalement, il existe un ensemble de pays où le travail à distance n'a pas été développé. Parmi ceux-ci le Bénin, la Suisse, le Maroc et la Colombie disposent déjà de projets et même d'une législation applicable à sa mise en œuvre. D'autres comme la Lituanie, la Côte d'Ivoire et le Sénégal, n'ont pas développé un système de télétravail.

Question n°2 :

Aspects liés à l'utilisation professionnelle d'outils informatiques. De quels types d'outils numériques les juges administratifs disposent-ils pour les aider dans leur travail (outils de recherche de jurisprudence, bases de données, logiciel d'appui à la rédaction des décisions, …) ?

Sur ce point, plusieurs pays de l'Association Internationale des Hautes Juridictions disposent d'outils de consultation des dossiers, documents, jurisprudences, tant au niveau externe qu'interne (Intranet), ainsi que d'un accès à des outils privés (payant) et même, dans certains cas, à des outils de rédaction de décisions et à des plateformes d'appui à la procédure dans son ensemble.

L'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Chili, la France, la Finlande, la Grèce, les Pays-Bas, le Portugal, le Mexique, la Norvège, l'Italie, Israël et la Turquie disposent de plateformes pouvant être utilisées comme bureau virtuel et permettant de consulter les dossiers et documents numérisés, la jurisprudence et, dans certains cas, d'accompagner toute la procédure jusqu'à l'émission de leur décision définitive.

En ce qui concerne la Cour Administrative Suprême de Thaïlande, les PC, les ordinateurs portables et même les tablettes sont à la disposition des juges administratifs dans l'attente de la mise en œuvre du système E-ADMINCOURT. Ce système permettra aux juges de travailler directement dans le système, y compris pour la rédaction des décisions.

Dans le cas de l'Espagne, les juges bénéficient de plusieurs outils, outre une page du Conseil Général du Pouvoir Judiciaire qui requiert un code de sécurité pour y accéder et où l'on trouve la jurisprudence, la législation et la doctrine.

Le Maroc, par sa base de données juridique, accède à un bulletin et à une base de données de dossiers judiciaires, ainsi qu'à un système d'assistance à la rédaction des décisions.

En République Tchèque, les juges peuvent utiliser la base de données de la Cour Suprême Administrative et les bases de données de législation et de jurisprudence pour consulter les affaires, la jurisprudence, etc.

La justice de Colombie dispose d'une série de ressources nécessaires à la réalisation de ses missions et envisage l'établissement d'un système de justice en ligne.

En Slovaquie, les procès peuvent être gérés en ayant recours aux outils ASPI (Wolters Kluwer) qui est un système automatisé d'information légale, Beck-online et Nextcloud qui permettent le partage de dossiers au sein d'une unité.

Les juges de Pologne exploitent des programmes spéciaux pour enregistrer les ordres judiciaires et les décisions émises, ainsi qu'un programme d'archivage.

La justice suisse utilise un système de recherche de jurisprudence du Tribunal Fédéral et un autre de consultation des articles et doctrines disponibles, ajoutés à un système de gestion qui permet de suivre la situation des dossiers.

Au Bénin, le dossier juridictionnel est archivé en ligne afin de pouvoir être consulté par le personnel du tribunal, grâce au paiement d'une souscription aux opérateurs de réseaux Internet. Par ailleurs, la justice du Bénin dispose d'un site Internet où sa jurisprudence est visible.

Un autre groupe d'Etats membres ne dispose que de bases de données de consultation de jurisprudence et de doctrine. C'est le cas de la Lituanie, qui utilise le système Infolex, base de données privée permettant de consulter la jurisprudence et les dossiers à laquelle peut souscrire n'importe quel avocat. Elle se trouve à disposition des juges administratifs et y sont visibles toutes les décisions anonymisées qui ont été rendues publiques.

De leur côté, le Luxembourg et la Suède disposent d'outils de recherche et de consultation de la jurisprudence nationale et européenne.

La Chambre Administrative de la Côte d'Ivoire exploite actuellement une base de données jurisprudentielle appelée « COMOE ». Elle dispose également d'une souscription au portail « Lexis Nexis » de droit public et aux versions électroniques des revues publiées par l'éditeur français Dalloz, AJDA (l'Actualité Juridique du Droit Administratif) et RFDA (Revue Française de Droit Administratif). La Cour du Sénégal est également abonnée à ces revues et a doté ses juges d'ordinateurs portables et de PC.

Question n°3 :

Aspects liés à l'utilisation professionnelle des outils informatiques. Comment est assurée la sécurité des outils informatiques de recherche et de travail à distance ?

Les Etats membres de l'Association Internationale des Hautes Juridictions Administratives ont mis en place des mesures de sécurité pour les outils informatiques de recherche et de travail à distance qui tiennent compte de la complexité desdits outils laquelle, comme nous l'avons vu, est variée. Cela va des procédures de sécurité les plus avancées – nécessitant un nom d'usager et un mot de passe en plus d'une signature électronique pour l'accès à leurs plateformes -, aux logiciels antivirus, protocoles SSL (Secure Sockets Layer / couche de sockets sûrs ; protocole pour navigateurs web et serveurs permettant l'authentification, le cryptage et le décryptage de données envoyées par Internet) et TLS (Transport Layer Security, version actualisée et plus sûre du SSL), en passant par des outils qui ne disposent que des mesures standard de n'importe quel hardware puisqu'ils ne comprennent pas de plateformes.

Parmi les Etats disposant de hauts standards de sécurité, se trouve la Turquie dont le système UYAP (Système National d'Informatique Judiciaire) requiert que les usages

soient affiliés à la Commission de Justice et disposent de signatures électroniques et mobiles. En outre, ce système requiert que l'usager et le serveur valident l'identité de l'un et de l'autre, que la connexion soit cryptée, qu'elle intègre le protocole SSL pour la sécurité de l'échange de données, ainsi qu'un logiciel anti-virus dans les ordinateurs des juges et des procureurs.

En France, les applications professionnelles telles qu'Ariane, Ariane Archives et le « Guide du Rapporteur » sont uniquement accessibles depuis l'Intranet du Conseil d'Etat, dont l'accès est protégé et s'effectue par l'intermédiaire d'un identifiant ou d'un mot de passe.

Au Mexique, la sécurité des systèmes du Tribunal Fédéral de Justice Administrative est basée sur la limitation de son accès et de son utilisation aux personnes dûment enregistrées, lesquelles ne peuvent y accéder que par leur nom d'usager, mot de passe et signature électronique, éventuellement, et information chiffrée.

Une situation similaire se présente en Allemagne, au Portugal et en Espagne, où, pour accéder au système et pour le télétravail, est en outre requise l'authentification au moyen d'une signature électronique.

Une autre catégorie d'Etats dispose d'organismes spécialisés dans l'application de la sécurité de l'information pour leurs tribunaux. Il s'agit notamment de la Finlande où la sécurité de la Technologie de l'Information en faveur des tribunaux est assurée par le Centre Gouvernemental de Technologie de l'Information et des Communications, Valtori, lequel fournit à l'Administration publique de l'Etat les services de TIC.

De même en Autriche, les demandes de la Cour Suprême Administrative (après paiement des frais y afférents), sont suivies par le Bundesrechenzentrum GmbH (BRZ GmbH ; Federal Computer Centre Ltd.) en qualité de fournisseur de services électroniques pour la Cour Suprême Administrative.

D'autres tribunaux ont des protocoles spéciaux, comme le Tribunal Administratif d'Australie, lequel dispose d'un Cadre de la Politique de Sécurité de Protection du Procureur Général (PSPF) afin de se protéger contre tout risque, vulnérabilité et menace de sécurité pour le Tribunal.

La plupart des juridictions administratives des Etats membres jouissent d'une protection basée sur l'authentification de l'usager à partir d'un nom d'usager et d'un mot de passe, en plus des systèmes anti-virus et de sécurité contre les attaques électroniques propres des systèmes numériques. C'est le cas des juridictions du Chili et de la Thaïlande, ainsi que du Canada, de la Corée, de la Norvège et du Maroc qui, par ailleurs, exigent l'authentification de l'usager en deux étapes pour accéder à leur plateforme. Même chose également pour la Hongrie dans le cas du bureau à distance de « la Curie » (Cour Suprême) auquel on accède à travers un VPN crypté suite à un processus d'identification à deux étapes ; pour le système d'accès restreint et d'accès à distance des tribunaux, seuls sont nécessaires le nom de l'usager et le mot de passe.

Concernant l'Autriche et la Pologne, il n'est possible d'accéder aux dossiers et aux archives judiciaires que depuis les ordinateurs portables et les PC autorisés par les services

de Technologie de l'Information des tribunaux. En Israël, pour entrer dans le système judiciaire, une carte intelligente est requise ou par le biais du service d'identification sécurisée du gouvernement.

Le réseau interne du Tribunal de Belgique est assuré à partir du début de session et un mot de passe tandis que le réseau externe est protégé par deux pare-feu qui fonctionnent simultanément.

La justice administrative de la République Tchèque a installé un logiciel anti-virus dans chaque PC ou matériel portable, le travail à distance ne peut s'effectuer qu'après autorisation du ministère de la Justice, sur demande de la Cour Suprême Administrative, par l'émission d'une carte avec certificat numérique et pour un temps limité.

Par ailleurs, il existe un groupe de juridictions où ont été mises en œuvre des mesures spéciales de sécurité au-delà des systèmes de sécurité anti-virus, comme c'est le cas en Colombie, qui est en passe d'installer une plateforme de travail en ligne, et en Lituanie et en Côte d'Ivoire dont les juridictions administratives n'ont, pour le moment, pas mis en place de mesures de sécurité spéciales, mais disposent d'une sécurité internet de base.

La justice du Bénin contrôle sa sécurité au moyen d'un logiciel anti-virus, tandis qu'au Sénégal la sécurité est assurée par du personnel du service informatique du tribunal.

Question n°4 :

Aspects liés à l'utilisation professionnelle des outils informatiques. Quelles sont les éventuelles conséquences disciplinaires en cas d'utilisation inadéquate des outils de travail numériques fournis par la juridiction ?

Pour ce qui a trait aux sanctions disciplinaires en cas d'utilisation inadéquate des outils de travail numérique fournis par la juridiction, nous remarquons, parmi les Etats membres de l'Association Internationale des Hautes Juridictions Administratives, que certains pays disposent d'une juridiction spéciale qui sanctionne ceux qui ne respectent pas les règles d'utilisation des outils numériques, et que d'autres appliquent les lois relatives à la responsabilité pénale et administrative applicables aux fonctionnaires lorsque ceux-ci méconnaissent les règles d'utilisation des outils numériques.

Dans le cas du Canada, les employés de la Cour Suprême sont soumis à la Directive de Technologie de l'Information, laquelle établit les usages acceptables de cette dernière au sein du Tribunal. Les membres du Tribunal Administratif Australien doivent, quant à eux, appliquer la politique sur l'utilisation et la sécurité des installations numériques.

Pour ce qui concerne la Chine, les départements de supervision intègrent la question de la sécurité du réseau dans le champ de leur supervision et pouvoirs d'inspection et enquêtent sur les responsabilités.

Dans le cas où un dossier électronique relatif à un jugement en ligne suivi auprès du Tribunal Fédéral de Justice Administrative du Mexique aurait été modifié, altéré, détruit ou qu'il aurait subi une perte d'information, ou qu'il serait démontré que le responsable a été un usager interne, le Tribunal introduirait une action en justice afin d'entamer une

procédure en matière de responsabilités administratives, sans préjudice de l'exercice de toute autre action légale à son encontre.

En Autriche, la Loi de Service, applicable aux fonctionnaires publics - à l'exception des juges fédéraux -, ainsi qu'aux employés engagés dans des institutions fédérales, contient certaines dispositions relatives à l'usage de la technologie de l'information et des communications (ICT - en français TIC) sur les lieux de travail.

Parmi les juridictions qui ont recours aux dispositions générales relatives à la responsabilité pénale ou administrative dans le cas d'une méconnaissance des règles relatives à l'utilisation des outils numériques, sont représentés l'Allemagne, le Bénin, la Belgique, le Chili, la République Tchèque, la Corée, la Slovaquie, l'Espagne, la Finlande, la France, la Grèce, l'Italie, Israël, la Lituanie, le Luxembourg, la Norvège, les Pays-Bas, la Pologne, le Portugal, le Sénégal, la Suède, la Thaïlande et la Turquie. Ces pays n'imposent pas de mesures disciplinaires spécifiques pour usage indu des outils numériques des juridictions, appliquant les règles générales relatives à la discipline des agents publics.

En Suisse, Côte d'Ivoire et Colombie, il n'existe aucune disposition spécifique sur ce sujet, ces pays étant dans l'attente de la mise en place du travail à distance et étant réglementés par la législation générale en matière de responsabilités.

/// SUJET 2

JURIDICTION ELECTRONIQUE

2.1] Juridiction Electronique (Contentieux Administratif en Ligne)

Question n°1 :

Votre juridiction a-t-elle la possibilité de traiter les affaires par voie dématérialisée ? Dans l'affirmative, quels sont les actes pouvant être accomplis de manière dématérialisée (saisine de la juridiction, échange de mémoires et de pièces, jugement, notification de la décision, …) ?

Sur ce sujet, les pays de l'AIHJA manifestent une réelle volonté de promouvoir un dépôt, suivi et résolution des procès administratifs par voie entièrement dématérialisée. Dans certains pays, les procédures électroniques coexistent encore avec les procédures traditionnelles sur support papier. C'est notamment le cas au Canada, en Chine, en Colombie, en Espagne, en Hongrie, en Lituanie, au Maroc, en Norvège, en République Tchèque, en Allemagne, en Australie, en Autriche, au Bénin, en Slovénie, en Finlande, en France, en Grèce, aux Pays-Bas, au Portugal, en Suède et au Mexique.

Parmi les nations qui disposent d'un système de gestion dématérialisée des affaires peuvent être mentionnés la Belgique, la Chine, la Hongrie, Israël, la Norvège, la Suisse, la Thaïlande, la Turquie, l'Australie, l'Autriche, le Chili, la Corée, la Finlande, la France, l'Italie, le Portugal et le Mexique.

La Pologne, l'Allemagne, la Slovaquie, le Luxembourg et le Sénégal sont sur le point de mettre en œuvre de tels dispositifs, qu'ils soient en cours d'adoption ou en cours d'expérimentation.

Dans les pays, comme le Canada, la Slovénie, la Grèce, les Pays-Bas, la Lituanie et la République tchèque, qui sont au nombre de ceux dont le cadre juridique prévoit l'utilisation des technologies numériques dans la fourniture du service de la justice, les documents, mémoires et actes procédures peuvent être déposés, reçus, consultés et reproduits par email, messagerie électronique, voire message texte. Les notifications ou autres communications sont également accomplies de cette manière.

Les pratiques vont d'un recours obligatoire aux outils numériques à une option facultative. Parmi les pays qui ont rendu obligatoire le recours aux outils numériques, comme l'Espagne, l'obligation pèse plutôt sur des groupes spécifiques comme les avocats ou les conseillers juridiques, mais pas sur le citoyen particulier. Cela concerne la Belgique, l'Espagne, la Norvège, l'Autriche et la France. La Côte d'Ivoire n'utilise pour l'instant pas de système numérique et toute la procédure juridictionnelle est assurée en présentiel.

Question n°2 :

Les preuves électroniques. Quelle valeur ont-elles ? ?

Il existe une tendance à l'utilisation accrue des preuves soumises de manière dématérialisée, que cela soit au stade pré-contentieux ou au cours de la procédure contentieuse elle-même.

En effet, la plupart des juridictions considère que les preuves et autres justificatifs transmis par voie dématérialisée sont recevables, y compris dans la procédure contentieuse. Il doit être souligné que les dispositions relatives à la recevabilité des preuves électronique sont généralement les dispositions de droit commun, même si la Suisse, le Bénin, la Corée du Sud et la Slovénie disposent d'une législation spéciale sur la manière dont les actes électroniques doivent être authentifiés.

Une question centrale s'agissant des preuves électroniques est celle de leur authenticité et origine. En Allemagne, pour qu'une preuve ou un justificatif soit considéré comme valide et authentique, il suffit qu'il soit téléchargé sur une plateforme dédiée au traitement des dossiers ou transmis via un système numérique spécialement créé à cet effet par un utilisateur dont l'identité a été préalablement validée et authentifiée. Dans d'autres pays, les documents sont complétés de l'information de la souscription avec signature électronique (Israël, Luxembourg, Norvège, Turquie, Allemagne, Pologne, Portugal, Sénégal et Mexique).

2.2] Sécurité des procédures juridictionnelles électroniques

Question n°1 :

Dossier juridictionnel électronique. Votre ordre juridique interne dispose-t-il d'un dispositif destiné à conférer les mêmes effets aux signatures électroniques qu'aux signatures manuscrites ? Si oui, dans quels cas ?

La règle générale au sein de l'AIHJA est qu'une signature électronique doit être vérifiée et comparée avec une signature papier pour être considérée comme valide.

En général, les règles relatives à l'utilisation des signatures électroniques incluent des règles relatives à l'usage de certificats numériques émis par des entités autorisées à le faire et qui confirment l'auteur, l'intégrité et la non corruption des données numériques du moment où elles sont transmises au moment où elles sont utilisées, avec parfois le recours optionnel à une technique d'encryptage. Cependant, certains Etats, comme la Côte d'Ivoire, la Chine, Israël, la Suède et surtout la Lituanie – dont l'ordonnancement juridique prévoit que les signatures électroniques ont la même validité qu'une photocopie et requiert que le document original soit présenté – ne reconnaissent pas la valeur légale de la signature électronique par rapport à la signature manuscrite ou refusent de les accepter dans certaines circonstances. De même, le Sénégal n'accepte pas l'utilisation de la signature électronique dans les affaires en relation avec la famille, les successions et la sécurité personnelle.

En général, toutes les parties au procès, et les juges, peuvent avoir recours aux signatures électroniques, sauf au Canada qui réserve l'usage de la signature électronique aux seuls juges tandis qu'en France les recours et les demandes auprès du Conseil d'Etat ne requièrent pas de signature électronique. Seule l'Espagne permet la signature électronique auprès de l'Audience Nationale, vu que ses procédures sont entièrement électroniques. Pour sa part, l'Allemagne admet les documents authentifiés par signature électronique et ceux authentifiés par une signature sur photocopie dès lors qu'ils sont transmis par un moyen de transmission sûr et prévu par la loi. La Finlande dispose d'une législation spéciale en la matière mais n'admet pas l'usage des signatures électroniques. Elle travaille toutefois sur ce point dans le but de mettre en place cette fonction.

Question n°2 :

La sécurité dans le dossier juridictionnel électronique. Dans l'hypothèse de procédures juridictionnelles dématérialisées, quelles sont les mesures mises en œuvre dans l'instruction du dossier électronique afin de garantir la sécurité des dossiers ?

Parmi les mesures de sécurité mises en place il est possible de mentionner les restrictions d'accès par type d'usager, l'interdiction d'installer, sur les disques durs officiels, des programmes ou des applications étrangères au système, le blocage de certaines adresses d'Internet, telles que celles qui correspondent à des réseaux sociaux et des sites peu sûrs, l'actualisation périodique des signatures électroniques et mots de passe, la migration des données des postes de travail vers des espaces de stockage plus sûrs, comme des serveurs centraux, l'utilisation des pare-feu pour éviter les fuites d'information, la réalisation de copies sécurisées transmises par des réseaux informatiques privés et la formation et sensibilisation des fonctionnaires et des employés sur les activités informatiques et leurs risques.

Certains aspects sont particulièrement surveillés tels que l'accès au système, lequel doit au moins prévoir deux étapes (par exemple, l'authentification de l'usager, à laquelle peuvent s'ajouter le recours à des codes ou des accès spéciaux pour la consultation des documents comme c'est le cas en Belgique). Garantir l'intégrité des données est une préoccupation constante, de telle sorte que l'intégrité des archives est assurée par leur conversion dans des formats ne permettant pas leur édition, avec la possibilité de placer des scellés (Canada et Thaïlande). La Chine, Israël et le Maroc ont recours à une gestion automatisée des documents, un contrôle des risques, un suivi des affaires, au cryptage de l'information et à des vérifications pour assurer la sécurité des données. La Suisse a recours à des plateformes de distribution. En Allemagne, au Chili, en Corée du Sud et en France il est possible d'inscrire les données dans un système et de les stocker pour une période de temps déterminée.

Parfois, certaines options supplémentaires sont disponibles pour les parties qui souhaitent vérifier l'authenticité des documents téléchargées sur la plateforme via Internet. En Corée du Sud, les données téléchargés sur la plateforme peuvent être comparées aux versions numériques conservées par les juridictions. En Espagne, lorsqu'il existe des doutes sur l'authenticité d'un document, les originaux et mêmes les images numériques peuvent être consultés directement.

Un des compléments pour atteindre la sécurité des systèmes est d'avoir recours aux réseaux privés permettant une communication entre les juges, les avocats et les tribunaux (Allemagne, Chili, Slovaquie, Slovénie, France, Grèce, Italie et Suède).

Question n°3 :

La transmission des actes procéduraux par voie électronique. S'agit-il d'un outil fiable pour la communication des actes de procédure aux intéressés ?

Quand les pays mettent en place des plateformes numériques, celles-ci permettent en général à la fois de recevoir et d'envoyer de l'information, soit par le biais d'une boîte aux lettres électronique, d'un courrier électronique ou d'un message texte incorporé au système. Dans d'autres situations, la notification s'effectue uniquement par l'utilisation d'un véhicule de transmission numérique, considéré individuellement, ne faisant pas partie à proprement parler d'un schéma intégré.

Le côté facultatif est persistant dans l'utilisation des moyens de communication électronique, mais il est obligatoire pour certaines personnes qualifiées, comme les avocats des parties. C'est le cas notamment en Belgique, au Mexique et en Chine où les notifications sont vérifiées par des échanges numériques sur la plateforme. Le Canada, qui admet l'envoi d'information par courrier électronique, continue en parallèle d'utiliser les registres sur papier. La Colombie permet l'utilisation de boîtes aux lettres électroniques, tandis que l'Espagne impose obligatoirement la notification électronique pour les professionnels représentant les parties. Israël privilégie la sécurité en envoyant séparément le document à partir d'un lien qui ne permet la récupération qu'après authentification.

L'Allemagne et le Mexique disposent chacun d'une plateforme de justice virtuelle qui fonctionne également avec un système de courrier électronique aux fins de communication sur l'avancement de la procédure. En Autriche, le dépôt d'un recours est également fait par voie électronique. La Corée du Sud indique que les notifications réalisées par le biais du système électronique sont considérées comme réalisées dès lors que le document a été consulté dans un délai d'une semaine après son envoi. Au-delà de ce délai, la notification est réputée avoir été effectuée. En Grèce, la notification électronique est limitée à la communication de décisions au Conseil Juridique de l'Etat. Aux Pays-Bas, les notifications et communications sont effectuées via le portail officiel du système plutôt que par messagerie électronique.

Au Portugal, le système informatique utilisé pour l'activité des tribunaux administratifs et fiscaux garantit la date et l'heure de l'envoi, fournit à l'usager une copie des documents envoyés avec la date et l'heure de leur présentation, et, dans le cas où la réception ne serait pas possible, produit un message informant d'une telle impossibilité. Le Sénégal a recours à des messages électroniques cryptés pour la transmission des actes aux parties dans les procédures juridictionnelles et, si des dispositifs périphériques de stockage sont utilisés, le code d'accès est envoyé séparément.

2.3] La responsabilité pénale et les moyens électroniques

Question n°1 :

Délits informatiques. Existe-t-il dans votre système juridique un délit de responsabilité pour dommages informatiques causés à l'administration ?

L'examen des codes et dispositions applicables aux juridictions administratives révèle que les pays membres ne prévoient pas de dispositifs pénaux particuliers pour les dommages informatiques causés à l'administration ou au sein de la justice administrative. En conséquence, la réparation du dommage éventuel sera gouverné par les dispositions de droit commun en matière de responsabilité civile extra-contractuelle.

Les manquements qualifiés de délits informatiques couvrent la violation de la confidentialité des systèmes d'information et les manquements aux règles d'accès à ces systèmes, la manipulation, détérioration et altération des systèmes et des plateformes de nature à compromettre la sécurité des systèmes numériques d'information en vue de commettre une fraude, d'obtenir des fonds illicites, de faire un usage illégal de données personnelles, de falsifier des documents authentiques et de violer ou modifier des équipements informatiques.

Les délits relatifs à la communication de l'information couvre la divulgation d'informations confidentielles ou l'incitation à leur divulgation, la fourniture illégale de services de certification de signatures électroniques, de services ou d'exploitation de services de cryptage, l'obtention illégale d'information par l'intermédiaire de faux liens Internet, la substitution de sites web, ainsi que la falsification de domaines. De même, sont sanctionnés le développement, l'entretien et la vente de matériel et d'applications informatiques permettant de commettre les actions ci-dessus mentionnées.

La Colombie, l'Autriche et l'Espagne ont des dispositions régissant les dommages causés aux systèmes informatiques de la fonction publique et du gouvernement. La Hongrie a adopté des dispositions qui sanctionnent sévèrement l'accès illégal par des agents publics aux archives et documents et la violation de confidentialité qui en résulte. Le Maroc, quant à lui, se réfère à deux délits : la divulgation d'information et l'accès non autorisé aux systèmes de traitement de données, y compris les données à caractère automatisé.

La Norvège sanctionne les dommages informatiques provoqués intentionnellement à l'administration publique. La Thaïlande, par une loi spéciale, sanctionne les dommages causés aux données ou aux systèmes informatiques qui créent un risque pour la sécurité publique, la stabilité économique et les infrastructures ou qui portent atteinte à l'intérêt général. Le Bénin sanctionne toutes les personnes, y compris les personnes morales, qui violent la sécurité des données informatiques ou commettent une fraude au moyen d'un système informatique ou d'un réseau de communication électronique.

Le Chili prévoit des sanctions pénales pour plusieurs délits perpétrés à l'encontre de l'administration, dont la destruction ou l'altération intentionnelle d'un système informatique, l'accès non autorisé à un tel système et la divulgation malveillante de données informatiques. En France, les dommages informatiques causés à l'administration ne sont pas couverts par la loi mais le Code pénal prévoit des sanctions aggravées pour les

personnes ayant occasionné un dommage aux systèmes de traitement automatisé des données gérés par l'Etat. Le Code pénal grec prévoit que toute personne qui, de façon indue ou abusive, copie, expose, utilise, divulgue ou enfreint une information ou des programmes informatiques constituant des secrets d'Etat, scientifiques ou professionnels, ou des secrets d'une entreprise du secteur public ou privé, est passible d'une peine d'emprisonnement d'au moins 3 mois.

Question n°2 :

Accès illégal aux systèmes. Comment sont réglementés les accès aux systèmes utilisés par l'administration ?

L'accès aux systèmes informatiques des juridictions administratives s'effectue, tel que mentionné auparavant, sur la base d'autorisations individuelles et/ou de groupe, avec l'emploi de mots de passe ou d'authentifications pour certaines actions, comme les signatures électroniques qualifiées et l'inscription et utilisation des données par les usagers. Pour l'octroi des accès, il faut tenir compte des profils des usagers, de telle sorte qu'ils n'ont accès au système que dans la mesure où c'est utile à l'exercice de leurs fonctions.

Les agents chargés de traiter les dossiers et de la résolution des affaires accèdent librement au système, tandis que d'autres doivent répondre à certaines conditions particulières pour y avoir accès. Le plus souvent, ces aspects sont régis par des dispositions internes des juridictions elles-mêmes. En plus des mesures visant à limiter l'accès illégal aux systèmes électroniques, au niveau des différents usagers qui les appliquent, il existe des protections générales sur les conditions d'utilisation du service, la conception des applications et des instruments techniques fournis par les technologies de l'information et des communications.

Il doit être relevé que le Portugal permet l'accès aux systèmes informatiques au moyen d'ordinateurs physiquement situés dans les tribunaux au moyen d'un code d'accès temporaire pour un maximum de quatre heures, après enregistrement et confirmation préalables de l'identité de l'intéressé. La même chose prévaut pour ceux qui dans une affaire particulière se voient autorisés à accéder aux mêmes lieux et ordinateurs pour une durée maximale de dix heures. Le Sénégal ne permet pas la consultation de la base de données de sa Cour Suprême autrement que par son personnel, mais son bulletin de décisions et d'information est en consultation libre. La Finlande permet un accès aux autres branches de l'administration, tandis que l'Espagne requiert des certificats électroniques délivrés par les autorités juridictionnelles.

Question n°3 :

La sanction pénale d'un délit informatique. En cas d'accès illégal au dossier juridictionnel avec violation de la confidentialité des données ou modification volontaire ou involontaire de leur contenu, quelles sont les sanctions pénales prévues ? Existe-t-il une sanction spéciale pour les agents publics dans l'hypothèse où ils seraient reconnus coupables d'avoir commis un délit informatique ?

Les peines et sanctions prévues pour ceux qui consultent illégalement les données conservées dans un système informatique ou violent leur confidentialité vont de l'amende à l'emprisonnement en passant par la suspension ou la saisie des instruments utilisés pour commettre le délit.

La Belgique et l'Autriche prévoient des sanctions spéciales pour les agents publics ayant commis de tels violations et ceux qui causent un dommage important aux infrastructures, définies comme les installations ou les systèmes essentiels au maintien des fonctions vitales de la société, la santé, la sécurité, le bien-être économique et social. Au Canada, les agents publics ayant fait un usage non autorisés des données informatiques dans le cadre de leur fonction se voient appliquer les mêmes sanctions que celles prévues pour les cas de fraude ou d'abus de confiance. La Colombie et la Turquie font partie des pays qui prévoient des peines aggravées quand le délit informatique est commis par un agent public, avec la suspension des fonctions le cas échéant. Le Bénin et la Slovénie prévoient également des des peines aggravées lorsque le délit est commis par le dépositaire d'une fonction publique.

De même, l'Espagne prévoit des sanctions aggravées lorsque le délit entrave la fourniture de services publics et porte atteinte au fonctionnement de l'administration. Tel que préalablement mentionné, la Hongrie, la Grèce et la Norvège prévoient des sanctions spéciales pour les agents publics causant un dommage à l'administration. Aux sanctions pénales d'amende et d'emprisonnement, la Lituanie prévoit également une peine de service d'intérêt général quand les moyens de protection des systèmes numériques sont endommagés.

Pour sa part, le Luxembourg signale la possibilité d'imposer des sanctions disciplinaires, malgré l'absence de sanctions pénales spécifiques pour les agents publics. La Thaïlande prévoit des sanctions spécifiques pour les agents publics et les membres de la police qui enfreignent la confidentialité et l'intégrité des données informatiques, volontairement ou involontairement. La Slovaquie, quant à elle, outre les critères classiques de la responsabilité pénale, requiert, pour pouvoir le sanctionner pénale, que l'agent public ait été au courant que l'accès n'était pas autorisé, c'est-à-dire que l'agent ait eu l'intention de commettre un délit.

La Finlande est un autre pays qui prévoit une peine aggravée lorsque l'usage inadapté d'un système d'information met en danger la fourniture d'électricité, la fourniture de prestations médicales, la défense nationale, l'administration de la justice ou toute autre fonction importante pour la société. De même, elle reconnaît la possibilité qu'un fonctionnaire public soit condamné pour avoir révélé un secret dont il avait connaissance en raison de ses fonctions. L'Italie mentionne l'existence de décisions en vertu desquelles des agents publics ont été condamnés pour violation de la confidentialité. Les Pays-Bas

soulignent aussi que les fonctionnaires publics, y compris les juges et les fonctionnaires légaux, peuvent être sanctionnés pour avoir rendu publics ou avoir divulgué des dossiers confidentiels. Au Portugal, la manipulation d'un système informatique dans le but de créer de faux documents ou de fausses données, s'il s'agit d'agents publics dans l'exercice de leurs fonctions, aggrave la peine d'emprisonnement.

/// SUJET 3

DEONTOLOGIE ET PROTECTION DES DROITS

Question n°1 :

Anonymisation des décisions de justice. Quelles mesures garantissent la confidentialité des données personnelles contenues dans les décisions de justice ?

Parmi les pays qui disposent d'une réglementation et/ou ont mis en place une technologie destinées à protéger la confidentialité des données il est possible de nommer la France, le Bénin et le Chili. Bien que la France, ait une politique de « données ouvertes », elle protège également dans une large mesure les données personnelles, tant des personnes physiques que des autorités impliquées dans une affaire donnée. Le Bénin fait de même. Le Chili a également développé un système numérique permettant d'assurer la confidentialité des affaires. En Autriche, ce sont les juridictions elles-mêmes qui procèdent à l'anonymisation des données quand elles sont mises à disposition du public.

La Corée n'anonymise pas les données relatives à ses agents publics. La Finlande et l'Australie ont une position similaire, considérant que les données personnelles pourront ne pas être publiées en fonction des circonstances. En revanche, ces deux pays publient le nom des juges ayant émis la décision. La Finlande choisit également d'anonymiser ces données sauf si une raison particulière justifie leur publication tandis que l'Australie anonymise ces données. En Slovaquie, le choix a été de limiter la divulgation de données personnelles, soit par décret soit par décision administrative. En Espagne, la loi organique sur l'organisation du pouvoir judiciaire, a prévu un pouvoir discrétionnaire vis-à-vis des données personnelles des personnes physiques avec la possibilité de n'autoriser l'accès qu'à une partie de la décision, mais de ne pas anonymiser les données personnelles dans les décisions relatives à des délits commis à l'encontre du Trésor public ou de l'Union européenne.

Le Mexique dispose de lois spécifiques en matière de transparence et d'accès à l'information publique. Il en découle que les décisions du Tribunal administratif fédéral doivent être éditées avant d'être rendues publiques : les données personnelles sensibles sont effacées à l'exception des noms et fonctions des représentants des autorités administratives à l'encontre desquelles les recours ont été formés. En citant, dans la version publique, le nom de la Chambre émettrice de la décision, il est possible de connaître l'identité des juges. Dans les versions publiques de référence, le nom des agents publics et leurs signatures physiques doivent apparaître. Les notifications réalisées à travers le Bulletin Juridictionnel ne sont destinées qu'aux parties au procès et doivent inclure le nom de la Chambre, le sens de la décision du magistrat, le nom du greffier en charge de l'affaire et, éventuellement, le nom du particulier demandeur.

Les pays suivants : Lituanie, Pologne, Italie, Grèce, Pays Bas, Thaïlande, Portugal, Suède, Hongrie, Israël, Chine, Maroc, République Tchèque, Norvège, Suisse (à l'exception des affaires dites « célèbres », c'est-à-dire celles qui sont largement couvertes par les médias) et Luxembourg ont tous la même position sur le fait de ne pas admettre la publication de données personnelles de personnes physiques (même si les Pays-Bas

permettent l'anonymisation de données pour les personnes travaillant pour une autorité administrative ou une entité légale, excepté pour les personnes physiques agissant comme mandataire).

De même, la Suisse, l'Italie, la Suède, la Grèce et les Pays-Bas publient les données personnelles des avocats, procureurs et défendeurs, ainsi que des publics, tandis que la Hongrie, la Norvège, la République Tchèque, la Chine et le Luxembourg, le font seulement pour les agents publics, bien que le Luxembourg publie de façon systématique ses décisions sur un site Web et que son Tribunal Constitutionnel et sa Cour de Cassation publient également, de manière complète et systématique, leur jurisprudence. Par ailleurs, dans des pays comme la Suisse, l'Italie et la Grèce, il existe la possibilité de solliciter l'anonymisation complète de l'information et parmi eux, seule la Grèce est en cours d'obtention d'une technologie protégeant les données personnelles. Le Portugal garantit l'anonymat à travers sa Division d'Organisation et d'Informatique.

Pour l'Allemagne et la Slovénie, les données des parties transmises à des tiers sont jugées confidentielles par excellence, à l'exception de celles qui concernent les agents publics, qui sont publiées. Le Sénégal ne dispose pas d'une réglementation en vue de maintenir la confidentialité des données personnelles, ces dernières étant publiées sur décision discrétionnaire de la Cour Suprême.

Pour les pays qui ne prévoient pas l'anonymisation de telles données, le particulier qui souhaiterait obtenir cette anonymisation devra en faire la demande expresse. Cela concerne la Belgique, le Canada et la Côte d'Ivoire. Par ailleurs, la Colombie estime que les parties doivent savoir qui seront leurs juges afin de garantir un procès transparent et légitime.

Question n°2 :

Utilisation des réseaux sociaux par les magistrats. Les magistrats peuvent-ils utiliser les réseaux sociaux et dans quelles conditions ? Quelles sont les règles qui le prévoient (loi, charte déontologique, …) ?

Certains pays disposent d'une réglementation spécifique sur l'utilisation des réseaux sociaux. Le Bénin dispose d'un code du numérique et la Slovaquie d'une loi sur les Juges et les Assesseurs qui prévoit que ceux-ci ont l'obligation de ne pas exprimer publiquement leur opinion sur les affaires en cours ou déjà jugées qui n'ont pas été conclues, ainsi que l'obligation de se comporter de manière honorable et éthique.

La France également possède une Charte de déontologie de la juridiction administrative, laquelle comporte plusieurs dispositions relatives à l'expression sur les réseaux sociaux. La Grèce dispose d'un Code d'Organisation des Tribunaux et d'une loi sur le Pouvoir Judiciaire qui déterminent les devoirs fondamentaux de ses membres et autorisent l'utilisation des réseaux sociaux à condition que cela ne contrevienne pas aux dispositions de ces textes. Il en est de même pour la Slovénie.

Le Chili a adopté une approche proactive sur l'utilisation des réseaux sociaux, celle-ci étant recommandée par la Cour Suprême. En Espagne, les magistrats peuvent, sur le fondement du principe de liberté d'expression, utiliser réseaux sociaux, y compris en

s'identifiant comme magistrats, mais à condition qu'ils ne contreviennent pas aux principes généraux de déontologie.

D'autres pays permettent aux magistrats et juges d'utiliser les réseaux sociaux. Il s'agit de la Pologne, la Lituanie, Israël, la Hongrie, la Colombie, le Canada, la Suède, le Sénégal, le Portugal, la Belgique, la Côte d'Ivoire, le Maroc, la République Tchèque, la Suisse, la Thaïlande et l'Autriche. Bien que ces pays ne disposent pas d'une réglementation spécifique sur l'utilisation des réseaux sociaux, ils prévoient la même possibilité que le groupe antérieurement mentionné se référant à la liberté d'expression et au fait que les magistrats ne peuvent contrevenir aux dispositions du Code de déontologie et doivent s'assurer que leur comportement demeure honorable en lien avec les positions officielles qu'ils occupent.

En Chine et en Belgique, il existe un document de la Cour et du gouvernement relatif à l'utilisation des réseaux sociaux, tandis que la Norvège et la Thaïlande considèrent le bon usage et l'éthique, sauf lorsque le bon usage contrevient à la loi et justifie alors des sanctions disciplinaires.

L'Allemagne et l'Australie restreignent l'utilisation personnelle, par leurs juges, d'un compte de réseau social et plus encore en leur qualité d'agents publics. De même, les Pays-Bas, bien qu'ils n'interdisent pas l'utilisation des réseaux sociaux, recommandent de ne pas y avoir recours ou de le faire de manière limitée. Au Luxembourg, qui ne dispose pas d'une réglementation spécifique en la matière, le pouvoir judiciaire est tenu au respect de principes de déontologie lorsque ses membres font usage des réseaux sociaux. Finalement, la Finlande, l'Espagne et l'Italie prévoient que l'utilisation des réseaux sociaux ressort du libre arbitre des fonctionnaires.

Le Tribunal Administratif du Mexique n'interdit pas aux magistrats et autres personnels juridictionnels, l'utilisation personnelle des réseaux sociaux. Cependant, il existe une réglementation interne autorisant et réglementant leur utilisation. Indéniablement, les réseaux sociaux ne peuvent être utilisés comme un moyen d'obtenir des réponses transparentes sur des informations détenues par le gouvernement, c'est-à-dire que ce ne sont pas des moyens efficaces pour obtenir des informations l'état d'avancement d'une affaire, le sens d'une opinion judiciaire ou la décision de justice.

Question n°3 :

Les outils numériques sont-ils utilisés en tant que mécanismes de contrôle et de plainte visant les agissements inappropriés des magistrats ? De quelle manière ?

La République Tchèque, la Suisse, la Thaïlande, la Turquie, la Hongrie, Israël, la Lituanie, le Luxembourg, le Maroc, la Norvège, la Côte d'Ivoire, l'Espagne, la Suède, la Belgique, le Canada, le Portugal, la Grèce, la Finlande et la France ne disposent pas d'outils numériques pour les registres ni pour les plaintes. Le Canada, le Portugal, la Finlande, la Pologne, le Maroc, la Turquie et la France utilisent comme unique instrument le courrier électronique tandis que l'Espagne n'utilise que les contrôles appliqués par rapport au nombre de dossiers.

D'autres pays, comme le Chili, ont recours aux outils numériques dans un tel contexte et notamment dans le cadre de poursuites disciplinaires, c'est-à-dire pour le dépôt et l'instruction de plaintes à l'encontre des membres du pouvoir judiciaire et pour y répondre. De même, la République de Corée utilise un site web de la Cour Suprême pour présenter des rapports ou des plaintes sur des actions inappropriées, un ombudsman (défenseur du peuple) en ligne et un réseau interne pour que les membres des juridictions informent de toutes les actions réalisées qui seraient contraires à la déontologie.

La Slovénie est favorable à l'utilisation d'outils informatiques tandis que l'Italie dispose d'un système informatique capable de traiter des données statistiques complexes et de garantir un suivi précis des retards dans le traitement des affaires et le rendu des décisions. Aux Pays-Bas et en Colombie, la conduite des employés des juridictions, leurs accès aux sites internet et les informations qu'ils transmettent et reçoivent sont contrôlés. La Chine, quant à elle, gère un système de contrôle et de prévention des risques, un système d'inspection automatique de preuve, ainsi qu'un système d'évaluation.

S'agissant du Mexique, les outils informatiques ne s'utilisent que comme mécanismes de contrôle statistique des affaires en cours. Ces outils ne permettent pas de déposer ou de répondre à des plaintes pour conduites inappropriées des magistrats. Cependant, il est possible que ces outils soient utilisés pour de telles procédures dans le futur lorsque les conditions seront réunies et que les procédures adéquates auront été adoptées. Dans l'attente, les plaintes sont déposées et traitées en version papier.

COMPTE-RENDU DES TRAVAUX EN COMMISSION

RAPPORT DE LA COMMISSION SUR L'IMPACT DES TECHNOLOGIES INFORMATIQUES SUR LES JURIDICTIONS ADMINISTRATIVES

Participants :
Australie, Belgique, Bénin, Chine, Finlande, Grèce, Italie, Mozambique, Pologne, Sénégal, Suisse, Thaïlande, Turquie.

Président :
M. Ousmane Batoko, *Président de la Cour suprême du Bénin*

Rapporteur :
M. Yunus Emre Yilmazoglu, *Senior rapporteur*

Après son discours d'ouverture, M. He Xao Rong, de la Cour suprême populaire de Chine, a pris la parole pour une présentation au cours de laquelle il a donné un aperçu détaillé des divers outils numériques dont la Chine dispose dans les procédures juridictionnelles, y compris plusieurs exemples tels que le dépôt électronique des affaires, la présentation de preuves liées aux dossiers, les audiences vidéo, la demande de micro tribunal mobile pour suivre la procédure à distance et la recherche de jurisprudence. Il a également mentionné l'utilisation d'Internet pour renforcer la transparence en publiant toutes les activités qui se déroulent dans les juridictions. Enfin, il a fait part de quelques statistiques importantes sur la numérisation des procédures judiciaires en République populaire de Chine. Il a notamment mentionné que la Chine avait construit une base de données regroupant 2 millions de jugements.

A l'issue de cette présentation, les membres de la commission n°1 ont entamé la discussion sur le premier cas pratique.

La première question abordait la portée du principe de « *bis de eadem re ne sit actio* », qui interdit la duplication des actions, dans le contexte où les juges ont accès à une base de données numérique permettant de faire des recherches et des recoupements à partir de plusieurs types de données (nom du requérant, nom du défendeur, lieu du litige, nom des juges…). Chaque pays a fait des remarques sur l'application de ce principe dans sa juridiction et, le cas échéant, a donné des informations sur les modalités d'examen de la recevabilité des affaires. Par la suite, les délégués des pays ont discuté du sujet de savoir à qui il incombe de vérifier si plusieurs affaires ont été déposées sur le même sujet. S'agit-il du demandeur ou du juge qui dispose d'un accès à une base de données numérique permettant de faire des recherches par noms des requérants, type de décision, etc. ? Les délégués ont également discuté des conséquences et des sanctions en cas de duplication des actions.

Plusieurs représentants (Belgique, France, Grèce, Bénin) ont mentionné que la recevabilité d'une affaire est un moyen d'ordre public devant être soulevé par le juge et auquel les parties ont la possibilité de répondre en présentant des observations. Ainsi, l'irrecevabilité d'une affaire, soulevée d'office par le juge sur la base des recherches effectuées sur la base de données numérique, devrait faire l'objet d'une notification préalable aux parties pour qu'elles puissent présenter des observations. Dans ce contexte, le représentant de la Slovénie a également soulevé la question de savoir s'il s'agit d'un droit ou d'une

obligation pour le juge de vérifier si plusieurs actions ont été introduites. Il a précisé que les outils informatiques sont à la disposition du juge, qui peut facilement voir s'il y a eu plusieurs actions. Et, en cas de manquement, l'affaire peut faire l'objet d'un appel. Sur la base de cet argument, les participants ont mentionné l'expérience de leur pays en matière d'utilisation des outils informatiques et les avantages qu'ils en tirent. Il était entendu que les pays de la Commission n°1 utilisaient les outils informatiques pour publier les décisions des tribunaux sur leurs sites web, vérifier les actions en double, rechercher la jurisprudence pertinente pour le recours dont ils sont saisis et suivre la jurisprudence pour assurer la cohérence et permettre la communication entre les tribunaux à des fins de cohérence.

Les délégués ont ensuite abordé la deuxième question qui s'interrogeait sur le fait de savoir s'il était possible ou acceptable qu'un juge utilise des outils informatiques pour rechercher des décisions en se basant sur le nom des parties, le montant demandé et le nom des juges, etc.

Les principaux concepts discutés dans ce cadre couvraient la transparence, la confidentialité et les limites de la confidentialité dans chaque pays. Il a été souligné que le juge, avec les outils disponibles, peut rechercher la jurisprudence en utilisant les mots clés pertinents pour chaque critère de recherche.

Une question très importante qui a été soulevée au cours des discussions a été la confidentialité des bases de données disponibles, ainsi que la publication des décisions. Sur la base du droit à la protection de la vie privée, l'anonymisation des décisions de justice et la protection des données personnelles ont été identifiées comme des exigences essentielles ayant toutes deux une signification particulière dans le cas des groupes vulnérables tels que les enfants, les femmes et les réfugiés. L'anonymisation des décisions peut être effectuée soit automatiquement par le tribunal, soit à la demande des parties. Dans les affaires administratives, lorsque l'État est le défendeur, il peut également être nécessaire de ne pas divulguer le nom de l'agent public qui a pris l'acte au nom de l'État afin de le protéger. Les discussions ont révélé qu'il existe différentes pratiques nationales concernant l'anonymisation du nom des juges. Dans certains pays la publication du nom des juges est une exigence constitutionnelle, tandis que d'autres pays se sont attachés à garantir un équilibre entre l'exigence de transparence associée au service public de la justice et la protection des juges contre les menaces dans certains cas particuliers liés aux spécificités d'une affaire. À cet égard, certains représentants ont souligné qu'il est nécessaire de connaître le nom des juges et de la juridiction à l'origine de la décision ainsi que toute opinion dissidente, ce qui a conduit les représentants des pays à discuter de la procédure d'audience publique et des affaires pour lesquelles les audiences peuvent se tenir à huis clos. Il a été relevé que les huis clos se justifiaient particulièrement dans les affaires relatives aux enfants et aux réfugiés. Les litiges fiscaux ont également été mentionnés. Sur ce point, il a été indiqué que le principe de l'audience publique est communément reconnu comme étant la règle mais que, dans certains cas, comme pour la protection des secrets commerciaux, les parties peuvent demander des audiences à huis clos, qui seront alors décidées par le juge. En Slovénie, depuis une modification de la loi, il est obligatoire de mentionner les noms des juges de la Cour suprême qui ont statué sur l'affaire et la manière dont ils ont statué dans les jugements civils et administratifs, ce qui signifie que les noms de ceux qui ont voté en faveur de la décision et ceux qui se sont opposés doivent être publiés. Cela peut poser des risques pour leur sécurité et entraîner l'impopularité des juges, notamment dans les affaires fiscales qui coûtent des milliers d'euros aux gouvernements.

La troisième question était relative à l'accès des parties aux bases de données.

Il ressort clairement des discussions que davantage de bases de données devraient être mises à la disposition des tribunaux. En ce qui concerne les bases de données dans lesquelles les décisions des tribunaux sont publiées, il a été constaté que certains pays préparent des versions publiques accessibles à tous. Il a été souligné que l'accès des parties aux bases de données est essentiel dans le cadre du droit à un procès équitable. Après des discussions détaillées sur les personnes qui devraient avoir accès au système et sur les informations particulières qui devraient être disponibles, il a été convenu en conclusion qu'il est important de mettre les bases de données à la disposition du public. Toutefois, dans certains cas, pour protéger les parties et le fonctionnement du système judiciaire, certaines données peuvent être omises ou occultées.

Ce fut la fin des discussions relatives au cas pratique n°1.

Le deuxième jour des discussions, le second cas pratique abordait les mécanismes de consultation du public.

Les principaux points de discussion étaient les suivants :

a] Les personnes physiques devraient-elles être les seules à pouvoir voter dans le cadre de la procédure référendaire ou les personnes morales devraient-elles aussi être autorisées à voter ?

c] Raisons d'une éventuelle limitation ?

c] Mesures visant à sécuriser la procédure de vote, telles que l'interdiction de voter plusieurs fois.

d] Conséquences juridiques des actes contre la sécurité de la procédure de vote, tels que l'annulation du référendum et l'annulation de la décision de l'autorité publique basée sur le référendum.

Il a été convenu par les délégués que lorsqu'une irrégularité est constatée lors d'un référendum non obligatoire, cela peut avoir des conséquences sur la légalité de la décision de l'autorité publique prise sur le fondement de ce référendum. Plusieurs délégués ont précisé que le vote ne serait attaquable que par le biais d'un recours dirigé contre la décision finale.

Certains pays ont déclaré qu'ils ne disposaient pas de la possibilité d'organiser des référendums pour consulter le public. Au lieu de cela, ils utilisent la procédure de la consultation ou d'autres procédures spécifiques comme dans le cas des questions environnementales pour lesquelles le public peut avoir à s'exprimer.

En ce qui concerne la conséquence possible de l'annulation du référendum, certains délégués ont souligné que pour être annulé, le résultat du référendum doit être substantiellement affecté par l'irrégularité constaté.

En ce qui concerne le champ des votants, certains délégués ont signalé l'importance d'ouvrir le vote aux personnes morales, tandis que d'autres se sont montrés plus réservés sur ce sujet. Dans le cas des personnes morales, c'est le représentant de la personne morale qui vote et non la personne morale elle-même. Par conséquent, l'opinion individuelle du représentant peut se refléter sur le vote, ce qui est l'une des raisons pour

lesquelles les personnes morales ne devraient pas être éligibles selon certains délégués. D'autres délégués ont soulevé le risque que des groupements de citoyens créent des associations d'opportunité uniquement dans la perspective de peser sur le vote. Enfin, certains délégués ont fait valoir qu'à partir du moment où elles ont un intérêt à agir, les personnes morales devraient pouvoir voter.

D'autre part, même si le référendum n'est pas obligatoire, il est l'expression de la volonté du peuple et, pour cette raison, des garanties procédurales doivent être prévues. En particulier, les principes généraux de transparence et de sincérité du vote doivent être respectés.

La deuxième question portait sur la sécurité du référendum. Il a été convenu par les délégués que le référendum serait annulé s'il devait être constaté que le système avait été piraté pour permettre à une seule personne de voter plusieurs fois. L'absence de garanties procédurales engendre une incertitude de nature à entacher le résultat d'irrégularité. En outre, la difficulté de prouver l'acte de manipulation lors du vote a été discutée, et il a été souligné une fois de plus que le vote est un moyen important d'expression démocratique et que sa sécurité doit être assurée.

Néanmoins, lorsqu'une irrégularité se produit et que le juge doit se prononcer sur ce point, il doit tenir compte à la fois de l'intérêt du demandeur à contester le référendum et de la volonté des électeurs. Dans le cas où l'irrégularité porte atteinte à l'exercice des droits démocratiques sans qu'il ne soit clairement possible d'en mesurer l'impact (nombre de votes concernés, etc.), l'annulation du référendum est envisageable.

La question 3 portait sur les conseils à donner aux autorités en vue de l'organisation d'un vote électronique pour un projet d'infrastructures. La plupart des délégués ont convenu qu'il n'était pas possible de donner des conseils en tant que juge. Cependant, dans certains pays, il existe des procédures permettant aux juges de donner des conseils dans des hypothèses bien précises.

Les délégués des pays dans lesquels il n'est pas possible pour un juge d'exercer une mission de conseil ont mis en évidence le principe d séparation des pouvoirs et ont ajouté que les autorités avaient toujours la possibilité de recourir à d'autres moyens tels que l'engagement d'un avocat, la recherche de la jurisprudence, l'analyse des dispositions juridiques connexes, etc. Tous les délégués ont néanmoins insisté sur le fait que la principale valeur à protéger devait être l'indépendance de la juridiction.

Dans les pays où il est possible aux juges de donner des conseils, la procédure garantit que l'avis fourni n'est pas celui d'un juge individuel mais un avis collectif de la juridiction. Dans le cas de la France, par exemple, lorsqu'une nouvelle loi ou règle entre en vigueur, le fait de donner un avis peut être utile pour l'interprétation de la nouvelle loi. Toutefois, si juridiction est saisie d'une affaire sur ce point précis, elle ne pourrait dispenser de conseils et des procédures de déport existent pour garantir l'impartialité.

Les discussions se sont terminées sur cette note pour la Commission 1.

Yunus Emre YILMAZOGLU
Rapporteur principal Juge de Sessions plénières de la Chambre de droit fiscal de le Conseil d'État de la République de Turquie

RAPPORT DE LA COMMISSION SUR LA JURIDICTION ÉLECTRONIQUE

Participants :
Belgique, Chine, Colombie, France, Israël, Mexique, Mozambique, Pays-Bas, Portugal, République De Corée, Thaïlande

Président :
M. Carlos Chaurand, *Président du Tribunal fédéral de justice administrative du Mexique.*

Rapporteur :
M. Yves Gounin, *Conseiller d'État, délégué aux relations internationales du Conseil d'État de France.*

Notre groupe comportait des représentants de 11 institutions représentatives des 5 groupes géographiques que compte notre Association : l'Europe, l'Afrique, le Moyen Orient, les Amériques et l'Asie. Avant de répondre aux questions qui nous étaient posées, une précision méthodologique et sémantique a été discutée sur le champ du sujet « la juridiction électronique ». De quoi s'agit-il ? Ce terme renvoie en fait à trois notions voisines mais distinctes. Seule la première de ces trois notions a été étudiée dans les questions qui nous ont été présentées. Il s'agit de la procédure électronique, de l'instruction électronique, des modalités selon lesquelles un requérant peut saisir, selon une procédure dématérialisée, la juridiction ; selon lesquelles il le peut, lorsque c'est une faculté, selon lesquelles il le doit, lorsque c'est une obligation. Entre aussi dans le champ de notre étude, les modalités d'échanges des mémoires entre le requérant, la ou le défenseur et les tiers intervenants, qu'ils soient appelés à la cause ou qu'ils interviennent de leur propre initiative. En revanche, deux autres notions, deux autres dimensions de la juridiction électronique n'ont pas été prises en compte, qu'on s'en félicite ou qu'on le déplore. Il s'agit de l'audience électronique, qui consiste, en dérogation au principe de l'audience physique, réelle, qui associe en un instant donné et en un lieu donné, les juges et les parties, à déroger à ce principe soit par la mise en place de vidéo conférences, soit, radicalement, comme c'est déjà le cas au Royaume Uni avec une audience entièrement électronique (ce sont les online dispute resolution). N'entre enfin pas dans le champ de notre étude la question du juge électronique, du robot, du juge qui peut se faire aider par des algorithmes d'intelligence artificielle pour, premièrement, rassembler des éléments de jurisprudence, deuxièmement, rédiger une partie, la plus factuelle, de son jugement, voire, là encore que l'on s'en félicite ou que l'on s'en inquiète, de l'aider à proposer des raisonnements conduisant à une solution. Nous nous focaliserons donc ici sur la procédure, ou, comme le disait notre collègue israélien Yigal Mersel, le e-filling.

Quatre remarques d'ordre général s'imposent.

La première wwest de constater que quelque soit le niveau de développement de nos pays, nous connaissons tous la mise en œuvre de procédures dématérialisées, certains pays étant plus avancés que d'autres.

Deuxième remarque, dans tous les pays cette mise en œuvre s'est faite progressivement. La dématérialisation ne se décrète pas, elle ne se fait pas d'un claquement de doigts, du jour au lendemain. Elle se heurte à des obstacles techniques. Elle se heurte à des obstacles psychologiques. Ces obstacles psychologiques d'ailleurs ne viennent pas tant des justiciables, ni tant des juges, que des avocats. D'où la mise en place, souvent, de ces procédures sous la forme d'expérimentation.

La troisième remarque, liée à la précédente, est celle que la généralisation de ces procédures n'est jamais absolue. Cette dématérialisation est obligatoire pour certains, elle est, et elle demeurera, a-t-on dit, facultative pour d'autres. Elle est obligatoire pour ceux qui sont en capacité de gérer ces instruments, de les manipuler : premièrement, les personnes publiques, deuxièmement, les parties disposant d'un avocat. Elle est encore facultative notamment pour les parties qui ne disposent pas d'un avocat, et ce dans toutes les institutions représentées dans la commission n°2 elle le demeure, même en Corée du Sud, qui nous avait fait, lors du Conseil d'administration de Venise il y a deux ans, une présentation particulièrement impressionnante, voire intimidante, de l'e-justice.

Quatrième remarque d'ordre général, inspirée par le poète français Alfred de Musset : « *Qu'importe le flacon, pourvu qu'on ait l'ivresse* », qu'importe que la procédure soit matérialisée, physique, papier, ou soit dématérialisée, c'est au fond les mêmes grands principes, les mêmes règles qui doivent s'appliquer. Ce point a été invoqué à plusieurs reprises par les représentants de Colombie, M. Valbuena, ou du Mexique. Les grands principes du contradictoire, d'administration de la preuve, continuent à s'appliquer identiquement aux procédures dématérialisées. J'ai cité Musset, j'aurais pu citer Giuseppe Tomasi di Lampedusa : « Il faut que tout change pour que tout reste pareil ».

Après cet élan lyrique, que j'espère vous m'aurez pardonné, j'en viens bien plus prosaïquement à l'examen des questions qui nous étaient posées.

CAS N°1

La première question concerne le régime des pièces présentées par un requérant sous une forme électronique.

Replaçons la question dans son contexte : nous sommes, dès lors que l'électronique est installée, face à une croissance exponentielle du volume d'une requête. Le coefficient multiplicateur de 10 a été évoqué par la représentante du Conseil d'État de France, Mme Catherine Bergeal : une requête est aujourd'hui 10 fois plus volumineuse qu'elle ne l'était avant. C'est bien compréhensible : là où, avant, peut-être une partie hésitait à fournir une centaine d'annexes parce qu'il fallait les imprimer, parce qu'il fallait les glisser dans une enveloppe, parce qu'il fallait timbrer l'enveloppe, aujourd'hui elle peut le faire en appuyant sur une touche, et elle ne s'en prive pas. Comment devons-nous réagir face à cette inflation ? C'est ici la question de la limitation de la taille des requêtes qui se pose. Limitation que l'on pourrait imaginer en nombre de pages, ou en nombre de caractères, d'octet, de kilo octets ou de giga octets. La mesure semble de bon sens et elle semble inéluctable pour venir à bout de cette inflation, mais elle se heurte à deux obstacles.

Le premier est d'ordre philosophique : n'y a-t-il pas une atteinte au principe de libre accès au juge qui figure dans beaucoup de pays soit dans la Constitution, soit dans un texte supra-national.

Deuxièmement n'y a-t-il pas une forme d'abstraction à vouloir fixer une limite qui vaille pour tous les types de contentieux ? Le président du Conseil d'État de Belgique, M. Jacques Jaumotte, citait le cas du dossier d'attribution du marché d'un avion de chasse qui rassemblait, et, a-t-il dit, c'était tout à fait normal et n'avait rien de choquant, des centaines si ce n'est des milliers de pièces. Il n'y aurait eu aucun sens à limiter ex ante le volume de cette requête-là.

Plus concrètement, la question n°1 soulevait la difficulté suivante : quid d'une pièce présentée par une partie qui serait illisible parce qu'elle n'est pas présentée dans un format électronique que la juridiction et les autres parties peuvent lire ? En fait, c'est un faux problème, a-t-on répondu, car, dans beaucoup de pays, on ne saisit pas le juge avec un courriel auquel on joindrait n'importe quel type de pièce jointe dans des formats électroniques obscurs. Le dépôt de la requête se fait sur une plateforme qui n'accepte que les pièces jointes qui sont enregistrées dans le format que la plateforme sait lire.

Deuxième difficulté, quid des requêtes auxquelles serait jointe une masse indescriptible d'annexes envoyée dans un désordre total ? Peut-on imposer que ces pièces soient indexées ? Que faire si elles ne le sont pas ? Opposer directement une irrecevabilité ? Non. La plupart des pays participant à la commission n°2 fait preuve d'un grand pragmatisme. La règle est la suivante : on n'oppose pas une irrecevabilité immédiate, mais l'on demande au requérant de régulariser sa requête en fournissant une table des matières dûment référencée des pièces jointes. C'est seulement si le requérant reste sourd à cette mise en demeure qu'une irrecevabilité est opposée.

Deuxième question : comment garantir l'authenticité des pièces ?

Nous avons eu un débat sur la signification de ce terme. Il ne s'agit pas de savoir si les pièces fournies sont bien authentiques, mais de savoir si c'est bien celui qui prétend les avoir déposées qui les a déposées. C'est la question du risque d'usurpation d'identité qui, à l'époque du papier, se réglait par la signature. La signature d'un papier attestait de l'identité de celui qui présentait ce papier. Quid, à l'ère électronique ? On aurait pu répondre que la signature électronique, similaire à la signature papier, permettait de répondre à ce défi, mais en fait, et c'est très intéressant, de nombreux pays ne recourent pas à la signature électronique et considèrent que l'identification du requérant sur la plateforme, grâce à son identifiant et à son mot de passe, suffit à garantir qu'il ou elle est bien celui ou celle qui a déposé la requête et les pièces qui y sont jointes.

Troisième question : comment gérer l'asymétrie électronique ? Comment faire si le requérant a déposé des pièces par internet et que le défendeur n'a pas accès à internet, dans des systèmes qui acceptent que la procédure dématérialisée reste facultative pour certaines parties ?

J'évoquais à l'instant le pragmatisme des différentes juridictions de la commission n°2, je devrais ajouter ici leur compassion, leur sympathie, vis-à-vis du tiers qui ne dispose pas d'accès à internet, car c'est dans beaucoup de pays le greffe du tribunal qui prend en charge cette asymétrie par deux procédures :

- la première, évoquée dans la réponse du Portugal, est de permettre à ce requérant de venir au tribunal pour avoir accès à un ordinateur et y consulter les pièces.
- la seconde, évoquée notamment par le juge Ahn de Corée du Sud, est d'imprimer les pièces de la requête et de les lui adresser par la poste gratuitement. C'est aussi le cas en France.

Voici pour le cas n°1.

CAS N°2

Le cas n°2 posait des questions de procédure qui s'inscrivaient dans la continuité de celle du cas n°1.

Que se passe-t-il si une partie considère que les pièces déposées par une autre partie sont irrecevables faute d'avoir été signées ?

La réponse à cette question figurait déjà en filigrane dans les réponses évoquées précédemment sur l'identification de l'identité du requérant dès lors que celui-ci est régulièrement inscrit sur la plateforme.

Je passe donc directement à la question suivante qui concerne les cas d'accidents techniques, de dysfonctionnements. *Quid* de la partie qui considère qu'elle n'a pas eu accès aux documents électroniques versés par une autre partie, parce qu'il y a eu une panne, ou parce qu'on ne lui a pas notifié.

La réponse est paradoxale et elle montre l'étonnante supériorité de l'électronique sur le papier. À l'époque du papier, il n'était pas facile d'administrer la preuve qu'une partie avait eu accès au papier. Avec l'électronique, dans le *brave new world* contemporain, tout est plus facile, parce que le tribunal, l'hébergeur de la plateforme, dispose des moyens électroniques de tracer les actions des différentes parties et de savoir si, contrairement à leurs allégations, elles ont eu accès à telle ou telle pièce.

Alors, s'il y a eu une panne, quelle doit être la réaction du juge ? Elle est la même que celle qu'il avait lorsque, à l'époque du papier, le moyen tiré d'une violation du principe du contradictoire était soulevé devant lui. Le juge va évaluer l'impact de telle ou telle interruption de service, dont il a connaissance car il dispose de tout l'historique des connexions des uns et des autres, sur le principe du contradictoire.

Que se passe-t-il s'il rejette l'argument et que la partie persiste dans son opposition et entend, après le jugement, soit dans l'appel qu'elle va former contre le jugement rendu, soit dans la requête en responsabilité qu'elle va introduire, se plaindre de ce que le juge n'a pas pris en compte un dysfonctionnement informatique ?

Ici, ce sont encore les règles traditionnelles de la responsabilité qui s'appliquent. Comme le disait M. Jacques Jaumotte, représentant de la Belgique, il faut, dans un système de responsabilité contractuelle, en cas de dysfonctionnement du service public de la justice, que trois éléments soient constitués : une faute, un préjudice, une relation de cause à effet entre la faute et le préjudice.

Les deux dernières questions, et je suis décidément beaucoup moins concis que le président Chaurand l'avait été avant-hier, concernent une hypothèse que nous avons tous connue dans notre vie : celle où tout à coup, en ouvrant notre ordinateur un écran noir s'affiche.

Dans ces cas là, on panique, premièrement, et puis au bout de 20 minutes de panique et d'énervement, on appel le service informatique. En général, une personne qui a l'âge de notre fils ou de notre petit-fils arrive, sans cravate et avec un chewing-gum, et en 10 minutes il retrouve le document qui avait disparu, et nous sommes tiraillés entre deux sentiments : une reconnaissance éternelle et la honte de ne pas avoir compris d'où vient le dysfonctionnement. Dans le monde du XXI^{ème} siècle, dans le monde informatique en effet, c'est miraculeux, un document ne disparait jamais tout à fait. Il existe toujours un double quelque part, et plusieurs pays sont intervenus pour souligner les efforts qu'ils ont consentis pour garantir la sécurité de leur système. Cela a suscité un débat intéressant sur la conservation des données électroniques. Un débat qui comportait deux volets.

Le premier est de savoir s'il ne faut pas à un moment détruire ces informations, si leur conservation sans limitation de durée ne violait pas la réglementation nationale ou supra-nationale sur la protection des données personnelles.

La seconde question que nous nous sommes posés, symétrique à la première, est celle de savoir comment conserver durablement ces documents. C'est le défi de l'archivage électronique, et je parle devant l'ancienne directrice des archives de France, qui est maintenant ma supérieure hiérarchique et donc je suis prudent.

La question se pose enfin du point de vue juridique. Que se passe-t-il si cette disparition électronique a été à l'origine d'un acte malveillant, commis par exemple par un agent de greffe ? Dans ce cas là, ce sont les principes du code pénal qui s'appliquent, c'est le cas en France comme dans d'autres pays. Le code pénal sanctionne la destruction volontaire de traitements automatisés par des peines d'amendes voir de prison. Les peines sont aggravées s'il s'agit de traitements automatisés de l'État, et, dans certains pays, elles sont une seconde fois aggravées si l'auteur de ces infractions est un fonctionnaire ou un agent investi de prérogatives de puissance publique. À ces sanctions pénales doivent être combinées des sanctions disciplinaires : il est probable et sinon certain que le fonctionnaire qui aurait commis de telles malversations soit licencié.

✳ ✳ ✳ ✳ ✳

Pour conclure, j'aimerais souligner deux points. Nos pays sont à des stades de développement très différents, connaissent des infrastructures électroniques et des taux d'équipement plus ou moins importants, mais tous partagent la même préoccupation et sont partis d'un même processus, celui d'une mise en place progressive de procédure dématérialisées. Nous appliquons tous des principes communs, le principe de pragmatisme, premièrement, et le souci de protéger le droit des justiciables. L'électronique n'est pas là pour compliquer les choses, il est là pour les simplifier.

Je vous remercie.

RAPPORT DE LA COMMISSION SUR DÉONTOLOGIE ET PROTECTION DES DROITS EN MATIÈRE NUMÉRIQUE

Participants :
France, Mexique, Thaïlande, Sénégal, Espagne, Chili, Italie, Côte D'ivoire, Suisse, Colombie

Président :
Mme Florence Aubry Girardin, *Juge du Tribunal Fédéral suisse*

Rapporteur :
M. German Bula Escobar, *Membre du conseil d'Etat de Colombie*

Le sujet de la commission est ouvert, car il aborde la question de la déontologie comme une question centrale. Les sessions de la table ronde ont porté sur des cas pratiques concernant le comportement des juges, qui étaient en même temps des professeurs d'université. Ainsi, la distinction entre le domaine académique et le champ juridictionnel a été examinée. Et des sujets intéressants ont été identifiés, qui peuvent être regroupés comme suit :

A] Aspects communs entre les différents pays lorsqu'un juge agit dans le domaine académique

1. Il est admis que les juges enseignent à l'université. Et il est entendu qu'il existe une liberté d'enseignement et d'expression. Les universités ont également leurs propres codes de conduite en matière d'enseignement.

2. Il est entendu que les juges-enseignants peuvent être critiques à l'égard de la jurisprudence, en termes académiques et juridiques.

3. Dans chaque cas, l'intention qui sous-tend la divulgation ou la critique des décisions judiciaires peut et doit être distinguée afin de différencier la pratique académique d'autres matières qui peuvent être censurées.

4. La divulgation des affaires judiciaires en cours n'est pas autorisée. Les informations qui peuvent être fournies doivent se référer à des affaires clôturées.

5. Les déclarations concernant des affaires en cours peuvent provoquer la récusation du juge.

6. Il existe des lois sur la protection des données, qui doivent être respectées par les juges-enseignants.

7. Les mineurs, les questions qui touchent à la vie familiale, les victimes de certains crimes et les questions privées sur la santé personnelle font l'objet d'une protection plus ou moins étendue et par des moyens différents.

8. Les considérations ci-dessus s'appliquent également aux juges qui écrivent des articles pour des revues et des journaux universitaires.

9. Certaines recommandations soulignent que, dans tous les cas, quiconque écrit ou donne une opinion oralement, ou en classe, doit préciser son statut de juge.

10. En ce qui concerne les étudiants participant à un stage, il a été souligné qu'ils partagent le devoir de protéger et de ne pas révéler des informations, tout comme un juge-enseignant.

B] Aspects communs entre les différents pays en matière de compétence

1. Il existe des lois sur la protection des données, qui doivent être respectées par les juges.

2. Il existe des mécanismes de rapporteurs pour effectuer la divulgation. Selon la jurisprudence de chaque pays, ces rapporteurs seraient chargés de traiter les informations qui sont proposées, et donc de les rendre anonymes, le cas échéant et selon les besoins.

3. Les arrêts sont publiés sur le web, ainsi que d'autres informations qui contribuent à la transparence (calendrier de l'activité judiciaire, etc.).

4. Il est reconnu qu'il existe des tensions entre le besoin de transparence et de publicité, d'une part, et l'obligation de protéger les informations sur les personnes, d'autre part. Il est reconnu que la publicité est implicite pour des raisons de procédure et de droits des usagers de la justice. Et, par conséquent, il est également reconnu l'existence de zones d'ombre.

5. Les difficultés pratiques de l'anonymisation sont également reconnues.

6. Les organisations de la société civile, ainsi que les institutions des différentes branches du pouvoir public, demandent généralement des informations sur l'activité judiciaire et sur le système judiciaire, et assurent le suivi des conduites et des positions jurisprudentielles.

7. L'utilisation des TIC et des réseaux par le pouvoir judiciaire n'est pas réglementée ; il suffit de respecter la loi sur l'habeas data. Les problèmes concernant la protection des informations sont reconnus dans les procès en ligne.

8. En tout état de cause, il est souligné la valeur de la transparence comme pôle de tension, et l'importance d'établir la confiance et la légitimité de la justice.

9. Les tribunaux ont pour pratique courante d'avoir des porte-paroles officiels, généralement ceux qui exercent la présidence de l'institution.

10. En ce qui concerne le secret des débats judiciaires, il est reconnu l'importance de la liberté d'expression et des changements d'opinion du pouvoir judiciaire, et comment cela génère des tensions par rapport à l'effet positif que la publicité des débats judiciaires pourrait avoir à l'égard des citoyens.

11. Les fondements communs de la responsabilité découlant du manquement à la protection de l'information des personnes ont été passés en revue, et il a été reconnu la nécessité de dériver cette responsabilité dans chaque cas spécifique, afin de distinguer celle du juge de celle qui incomberait à ceux qui effectuent la diffusion par quelque moyen que ce soit (en particulier Internet et les réseaux sociaux).

12. La nécessité d'avancer dans la clarification du champ d'application et des modes concrets de protection de l'information a été reconnue, dans la mesure où il existe une diversité notable de pratiques, de réglementations et de zones grises.

13. L'importance cruciale de l'éthique personnelle de chaque membre du pouvoir judiciaire a été soulignée, en particulier à une époque où les nouvelles technologies impliquent la diffusion immédiate et mondiale de l'information.

14. L'utilisation d'un porte-parole par les tribunaux contribue à éviter la falsification technologique de déclarations qui peuvent être facilement attribuées aux juges d'aujourd'hui. Le contrôle est plus compliqué si la voix du tribunal est diffusée.

15. La nature particulière des réseaux sociaux a été reconnue, ce qui permet l'émergence de conflits et de débats dans lesquels le pouvoir judiciaire pourrait s'impliquer, et il a donc été admis qu'il fallait faire preuve d'une extrême prudence quant à l'utilisation des réseaux sociaux. Il convient d'éviter tout type de participation à des procès que l'on tente parfois de mener en ligne.

16. Dans le même temps, il a été reconnu que les TIC et les réseaux sociaux peuvent être utiles et positifs pour l'activité judiciaire et pour renforcer la transparence et la confiance dans les institutions judiciaires.

17. Il a été souligné l'importance de reconnaître chaque juge comme porteur des droits des citoyens, et l'absence de juges dont la vie et les opinions pourraient être exigées comme neutres afin d'être considérés comme impartiaux au moment de prendre des décisions juridictionnelles. Les décisions judiciaires sont prises, conformément à la loi et pour le peuple ; ce ne sont pas des décisions personnelles.

18. Il a été fourni des informations sur les droits contemporains, issus de la loi et de la jurisprudence, concernant l'habeas data, comme la mise à jour et l'élimination des informations des bases de données et des réseaux.

C] Autres considérations communes

1. En général, et selon différentes modalités, il est considéré comme inapproprié d'exprimer des avis négatifs sur les décisions de la bourse. Il est considéré comme allant de soi que les fonctions de boursier sont remplies. Les décisions appartiennent au boursier.

2. La liberté d'expression est considérée comme allant de soi, mais aussi, dans le même temps, le devoir de respecter la bourse, ainsi que le devoir d'assurer la confiance dans la justice et sa dignité.

3. Sous différentes formes - juridiques ou disciplinaires -, il existe des sanctions pour les juges qui portent atteinte à la dignité de la justice ou qui agissent contre la bourse (dans certains pays, il est expressément stipulé que les juges durent tant que leur bonne conduite existe). A cet effet, dans chaque pays, il existe des institutions chargées de juger les affaires correspondantes (Collèges de déontologie, Conseils de la magistrature, Tribunaux de déontologie, etc.)

4. En aucun cas, il n'est admissible qu'un juge dise ou laisse entendre que le jugement qu'il critique est médiatisé par la corruption. Dans ce cas, tous les pays exigent des plaintes spécifiques et le juge peut être poursuivi pour défaut de signalement.

5. Le rôle des médias a été évoqué : la divulgation ne nécessite que le respect de la loi sur l'habeas data. On sait que les médias peuvent jouer et jouent un rôle complexe en ce qui concerne les procédures et les décisions judiciaires.

6. D'une manière générale, la nécessité de revoir les relations du pouvoir judiciaire avec les médias est reconnue. La seule réforme substantielle du Code de conduite de Bangalore (2004) vise précisément à moderniser ces relations ; mais la question admet un débat et une élaboration plus approfondis.

7. Des différences sont reconnues entre la divulgation traditionnelle des jugements et leur consultation physique au secrétariat du tribunal, et l'utilisation d'Internet et des réseaux sociaux.

8. L'importance du débat sur l'opacité entourant la gestion des grandes données a été reconnue.

D] Différences importantes à souligner

1. Certains pays (France, Espagne) pratiquent l'anonymat en règle générale.

2. Dans certains cas (France), l'anonymat s'étend même aux personnes morales. La dissociation inclut également les avocats, les cabinets d'avocats et les fonctionnaires administratifs dont les actes ou les décisions sont soumis à un contrôle juridictionnel. Elle vise à éviter de laisser une trace d'identification des questions, dans le but de protéger les personnes.

3. Une distinction est faite entre les degrés d'anonymisation. Dans un degré profond, il est interdit de proposer des données permettant d'établir des corrélations et d'identifier, de cette façon, les personnes concernées.

4. Dans certains pays, il existe un débat sur la dissociation du nom du juge, compte tenu du phénomène du terrorisme et de la sécurité et des droits des fonctionnaires du pouvoir judiciaire.

5. Bien que la préoccupation soit commune, il existe différents traitements au problème de l'information du juge, en ce qui concerne la protection contre le terrorisme.

6. Une annotation a été faite en ce qui concerne la capacité de la criminalité à disposer d'informations sur les juges, les détails de l'affaire, etc.

7. Dans certains pays, l'anonymisation de la signature autographe du juge a également été proposée.

8. Dans la plupart des pays, les discussions présentées lors des réunions des plus hautes juridictions sont secrètes.

9. Certains pays (le Mexique - certains sont télévisés - et la Suisse, dans des cas spécifiques, et sans télévision malgré les pressions législatives) tiennent des audiences publiques dans lesquelles, par conséquent, l'anonymat n'est pas possible.

10. Pour la plupart des pays participant à la réunion, l'anonymat est exceptionnel.

11. En fait, une sentence est prononcée avec une information complète (sauf pour les informations dont la loi exige la confidentialité). Et une fois qu'elle est émise, l'hypothèse de pouvoir contrôler sa non-publicité au-delà d'un certain point n'est pas plausible.

12. Dans ces derniers, il est habituel de faire la distinction entre différentes sources confidentielles :
    A. D'office - par décision judiciaire - (avec un appui juridique).
    B. A la demande d'une partie (avec l'appui de la loi).
    C. Obligatoire (personnes ou situations spécialement protégées par la loi).

13. Dans la plupart des pays, il est habituel d'expliquer par écrit une opinion dissidente, ainsi que la précision des nuances par rapport à la ratio decidendi (au moyen d'une opinion concordante).

14. L'Union européenne dispose de réglementations supranationales, mais la conduite de ses propres tribunaux n'est pas homogène (Luxembourg, Strasbourg).

15. Dans certains pays, il y a un débat : si les décisions administratives contentieuses concernent le secteur public, y aurait-il quelque chose à protéger ?

16. Certains secteurs d'avocats demandent l'anonymat.

17. Dans certains pays (Thaïlande), les citoyens peuvent signaler un comportement inapproprié sur le site web du tribunal.

18. Dans les cas de protection spéciale (mineurs), l'affaire va au-delà de l'anonymat, jusqu'à ce que le jugement ne soit pas publié.

19. Dans certains pays (Mexique, Colombie), l'administration, lors de l'envoi du dossier administratif au juge, peut demander ou informer le pouvoir judiciaire de la protection des données correspondante.

E] Déontologie, morale, éthique et conscience

- ❖ Au-delà de ce qui est prévu par la loi, les codes d'éthique, de conduite ou de déontologie, la réunion a mis en évidence le rôle des pratiques culturelles qui tournent autour des notions de déontologie, de morale, d'éthique et de conscience personnelle de chaque juge.

- ❖ Il existe une obligation de s'abstenir de tout comportement public qui porte atteinte aux valeurs et à la dignité de la justice.

- ❖ L'aspect déontologique est extrait de la loi, des règlements, des codes de conduite, des codes d'éthique et autres, et des pratiques culturelles.

- ❖ En général, il est clair que les juges ont des normes de conduite élevées, étant donné qu'ils ne peuvent pas dissocier cette condition de responsabilité en tant qu'agents publics judiciaires, de celle des citoyens ordinaires.

- ❖ Certains pays ont indiqué que leurs juges sont réfractaires aux codes éthiques écrits.

- ❖ En général, le rôle préventif crucial que les pairs jouent dans le contrôle des comportements inappropriés (soft power) est reconnu.

- ❖ Alors que le thème de la commission est encadré dans les questions générales de «*Open Government*» et «*Open Justice*», et compte tenu du fait qu'un bon nombre de pays membres de l'AIHJA font en même temps partie de l'OGP - Open Government Partnership, le représentant de la Colombie a proposé d'étudier une manière concrète de relation entre les deux organisations qui permette d'avancer dans les études et les débats sur ces sujets, avec la plus grande qualité possible.

NOTE :

Après la lecture du rapport précédent, les préoccupations et les interventions de la session plénière ont été entendues, ce qui permet d'ajouter le rapport comme suit :

- Dans tous les cas, il est recommandé aux juges et aux magistrats de ne pas entrer dans des controverses dans les réseaux sociaux, ou à travers les médias.
- Il est recommandé de maintenir et de renforcer la bonne pratique consistant à utiliser des communiqués de presse, en particulier en ce qui concerne les questions complexes, afin de communiquer de manière complète, claire et concise une décision judiciaire adoptée.
- Une prudence particulière est recommandée dans l'utilisation de formats restreints, afin d'éviter que certaines expressions ne soient sorties de leur contexte et utilisées à mauvais escient.
- Il est souligné l'importance cruciale et le rôle irremplaçable de la conscience de chaque juge, compte tenu de la rapidité des changements techniques et de leur impact sur l'information, la communication et les réseaux sociaux.

3

QUESTIONNAIRE

RAPPORTEURS

/// LE DROIT PUBLIC ET LES NOUVELLES TECHNOLOGIES DU NUMERIQUE

THEME 1 : IMPACT DU NUMERIQUE SUR LES JURIDICTIONS ADMINISTRATIVES

[SUJET 1] Environnement numérique en matière administrative

Question n°1 :
L'identification électronique. Existe-t-il un registre des fonctionnaires publics et des représentants légaux dans la législation nationale ? Dans l'affirmative, comment est-il réglementé ? Quelle est sa nature ?

Question n°2 :
Transparence et accès à l'information. Quelles sont les obligations des juridictions, en particulier administratives, en matière de diffusion de ses données et jugements (Open data) ?

Question n°3 :
La démocratie numérique. Votre pays a-t-il recours aux outils numériques pour l'expression de la volonté populaire (élections, consultations du public…) ? Si oui, comment le recours à ces outils est-il encadré ou contrôlé par le juge administratif ? Comment la sécurité de ces consultations est-elle assurée ?

[SUJET 2] Outils numériques et travail du juge

Question n°1 :
Aspects liés au télétravail. Les juges administratifs disposent-ils de la possibilité de travailler à distance ? Si oui, quels sont les outils numériques et informatiques mis à leur disposition (application spécifique, portail en ligne, VPN…) pour traiter les dossiers à distance ?

Question n°2 :
Aspects liés à l'utilisation professionnelle des outils informatiques. De quels types d'outils numériques les juges administratifs disposent-ils pour les aider dans leur travail (outils de recherche de jurisprudence, bases de données, logiciel d'aide à la rédaction des jugements,…) ?

Question n°3 :
Aspects liés à l'utilisation professionnelle des outils informatiques. Comment la sécurité des outils informatiques de recherche et de travail à distance est-elle assurée ?

Question n°4 :
Aspects liés à l'utilisation professionnelle des outils informatiques. Quelle sont les éventuelles conséquences disciplinaires en cas d'utilisation inappropriée des outils de travail numériques fournis par la juridiction ?

THEME 2 : JURIDICTION ELECTRONIQUE

[SUJET 3] La juridiction électronique (Contentieux administratif en ligne)

Question n°1 :
Votre juridiction a-t-elle la possibilité de traiter les affaires par voie dématérialisée ? Si oui, quels sont les actes susceptibles d'être réalisés par voie numérique (saisine de la juridiction, échange de mémoires et de pièces, jugement, notification de la décision…) ?

Question n°2 :

Les preuves électroniques. Quelle est leur valeur ?

[SUJET 4] Sécurité des procédures juridictionnelles dématérialisées.

Question n°1 :
Dossier juridictionnel électronique. Votre ordre juridique interne dispose-t-il d'un dispositif destiné à conférer les mêmes effets aux signatures électroniques qu'aux signatures manuscrites ? Si oui, dans quels cas ?

Question n°2 :
La sécurité liée au dossier juridictionnel électronique. Dans l'hypothèse de procédures juridictionnelles dématérialisées, quelles sont les mesures mises en œuvre dans l'instruction du dossier électronique afin de garantir la sécurité des dossiers ?

Question n°3 :
La transmission des actes procéduraux par voie électronique. Est-elle un outil fiable pour la communication des actes procéduraux aux intéressés ?

[SUJET 5] La responsabilité pénale et les outils numériques

Question n°1 :
Délits informatiques. Existe-t-il dans votre système juridique interne un délit de responsabilité pour dommages informatiques causés à l'administration ?

Question n°2 :
L'accès illégal aux systèmes. Comment est réglementé l'accès aux systèmes utilisés par la juridiction administrative ?

Question n°3 :
La sanction pénale d'un délit informatique. En cas d'accès illégal au dossier juridictionnel avec atteinte à la confidentialité des données ou modification volontaire ou involontaire de leur contenu, quelles sont les sanctions pénales prévues ? Existe-t-il une peine spécifique pour les fonctionnaires qui seraient reconnus coupables d'un tel délit ?

THEME 3 : DEONTOLOGIE ET PROTECTION DES DROITS

Question n°1 :
Anonymisation des décisions de justice. Quelles sont les mesures prises pour garantir la confidentialité des données personnelles contenues dans les décisions de justice ? Jusqu'à quel point est-il procédé à cette anonymisation (nom des juges, nom des greffiers, nom des parties, autres données susceptibles de révéler l'identité des parties…) ?

Question n°2 :
Usage des réseaux sociaux par les magistrats. Les magistrats peuvent-ils utiliser les réseaux sociaux et dans quelles conditions ? Quelles sont les règles le prévoyant (loi, charte de déontologie…) ?

Question n°3 :
Les outils numériques sont-ils utilisés en tant que mécanismes de contrôle et de plainte visant les agissements inappropriés des magistrats ? De quelle manière ?

RAPPORT GÉNÉRAL

LE DROIT PUBLIC
ET LES NOUVELLES TECHNOLOGIES INFORMATIQUES

2019

AIHJA IASAJ
Association Internationale des Hautes Juridictions Administratives