




# GENERAL REPORT

PUBLIC LAW AND THE NEW INFORMATION  
TECHNOLOGIES

**2019**

**AIHJA**  
**IASAJ**

**Association Internationale**  
**des Hautes Juridictions Administratives**



«En application de la loi du 11 mars 1957 (article 41) et du Code de la propriété intellectuelle du 1<sup>er</sup> juillet 1992, toute reproduction partielle ou totale à usage collectif de la présente publication est strictement interdite sans autorisation expresse de l'éditeur. Il est rappelé à cet égard que l'usage abusif et collectif de la photocopie met en danger l'équilibre économique des circuits du livre.»

© Direction de l'information légale et administrative. Paris 2021



**Editorial Board**

Martine DE BOISDEFFRE

President of the Report and Studies Section of the Council of State of France  
Secretary General of the International Association of Supreme Administrative  
Jurisdictions

**Editorial Director**

Marie LANORE

Head of International Relations of the Council of State of France  
Secretary of the International Association of Supreme Administrative Jurisdic-  
tions

## CONTENT

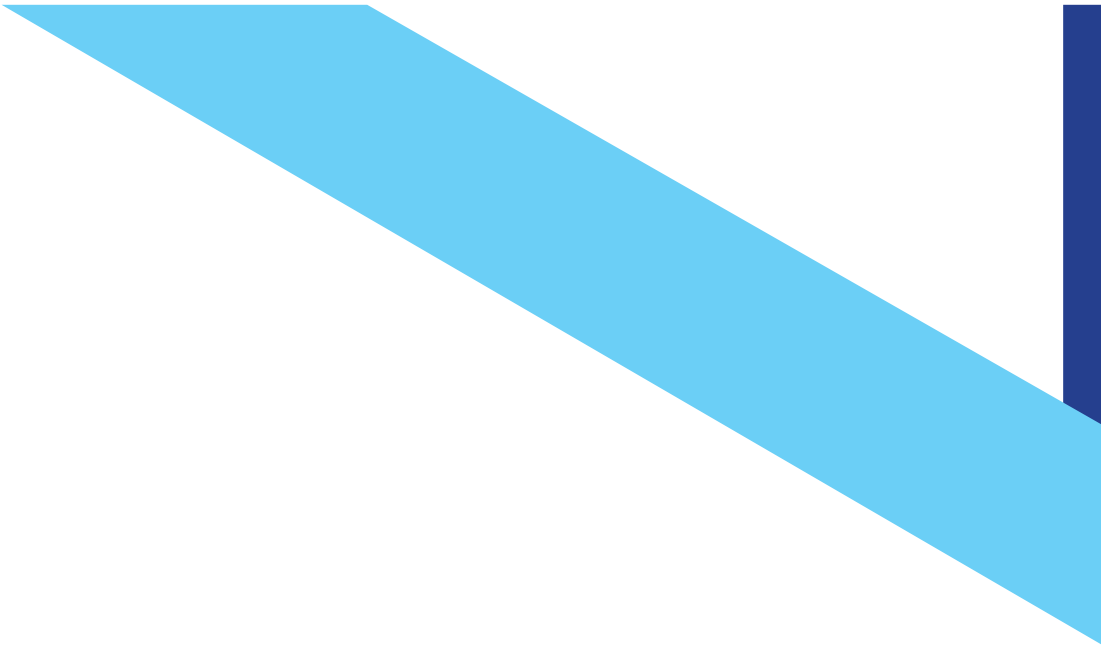
# 1 /// GENERAL REPORT

> <u>TOPIC 1</u>	
<b>THE IMPACT OF THE INFORMATION TECHNOLOGIES ON ADMINISTRATIVE JURIDICTIONS</b>	<b>10</b>
1.1] The digital environment in the administrative field	10
1.2] Computerized tools and judging	14
> <u>TOPIC 2</u>	
<b>ELECTRONIC JURISDICTION</b>	<b>20</b>
2.1] Electronic Jurisdiction (Online Administrative Litigation)	20
2.2] The security of online legal proceedings	21
2.3] Criminal liability and the electronic media	24
> <u>TOPIC 3</u>	
<b>ETHICS AND DATA PROTECTION</b>	<b>28</b>

## 2 /// MINUTES OF THE COMMISSIONS WORK

> REPORT BY THE IMPACT OF DIGITAL TECHNOLOGY ON THE WORK AND ORGANISATION OF ADMINISTRATIVE JURISDICTIONS COMMISSION	34
> REPORT BY THE ELECTRONIC JURISDICTION AND ONLINE LITIGATION COMMISSION	38
• Case n°1	40
• Case n°2	42
> REPORT BY THE ETHICS AND PROTECTION OF RIGHTS COMMISSION	44
A ] Common aspects between different countries when a judge acts in the academic field	44
B ] Common aspects between different countries with regard to the jurisdictional field	45
C ] Other common considerations	46
D ] Important differences to be highlighted	47
E ] Deontology, moral, ethics and conscience	48

## 3 /// QUESTIONNAIRE





**GENERAL REPORT**

# /// TOPIC 1

## THE IMPACT OF THE INFORMATION TECHNOLOGIES ON ADMINISTRATIVE JURISDICTIONS

### 1.1] The digital environment in the administrative field

#### Question n°1 :

*Electronic Identification: Does the national legal system have a register of public officials and legal representatives? If so, how is the said register regulated and what is its nature?*

The matter of whether there are registers of officials and legal representatives in the domestic legal system whereby administrators are able to find the names of public servants, along with their positions, profiles and functions, so as to ensure certainty in those subject to administrative proceedings and enable them to identify both the public servants who mandate and execute such proceedings and also the professionals who are legally empowered to represent private parties before public bodies is an important transparency issue for the public administrations of all countries.

Of the countries that belong to the **International Association of Supreme Administrative Jurisdictions**, we find that Colombia, Switzerland, Finland, Italy and Mexico have a national register of public servants and a public register of professionals.

For example, Switzerland, one of the countries that has both the aforementioned types of register, possesses a Federal Yearbook that can be consulted online by the public, and contains the names of the members of the Federal Assembly (i.e. Swiss parliament), the members of the federal courts (judges and court clerks), the members of the Federal Council and of the name of the Swiss Chancellor, along with the names, functions and contact data of the top federal civil servants and the main parliamentary officials and the senior staff of other important public-law institutions who perform administrative functions in the Confederation.

It also has a public register of legal representatives that contains information that each member of the Federal Assembly must make public upon taking up his/her position and subsequently at the beginning of each year.

Professional activities: if the member is an employee, s/he should specify:

- \* His/her position and employer.
- \* Which managerial, supervisory, advisory or other posts s/he holds in Swiss or foreign companies, institutions or foundations, whether private or in the area of public law.
- \* Which advisory or expert functions s/he performs on behalf of the Confederation.
- \* Which managerial or advisory functions s/he performs on behalf of Swiss or foreign interest groups.



\* Which functions s/he performs on committees or in other entities of the Confederation.

Greece and Benin have registers of public officials. The former has an electronic register of human resources which, among other things, contains information about all the members of the judicial branch, the staff of all the courts, and the representatives of the State Law Council, while Benin's Ministry of Labor and Public Administration produces an online file containing information about all civil servants and their performance.

Canada also has a register that contains information about federal public servants and their offices, which forms part of the National Online Directory of the Canadian Government, while information about lawyers appears in privately published directories rather than in public registers.

While Norway does not have a central register of public officials, each of its government departments keeps a list of its officials, as is also the case in Austria, China and France.

Germany, the Czech Republic, the Netherlands, Hungary, Poland and Portugal consider that the lists kept by their respective Bars constitute national registers of attorneys-in-fact.

Turkey has a very sui-generis system whereby professionals who wish to be registered with the Turkish Law Council — and exercise the rights that are contingent upon the said registration, which will be discussed below — must become members of the Turkish Union of Associated Bars.

Some of the Association's member countries, such as Belgium, Luxembourg, Korea, Slovakia and Lithuania, do not have such a register, while Thailand has a general population register, in compliance with its Law Governing Registration and Identification, but no register of public servants or legal representatives.

#### *Question n°2 :*

*Transparency and Access to Information: What are the obligations of the jurisdictions —especially of the administrative ones— with regard to the dissemination' of their data and rulings (i.e. open data)?*

Since private parties that appear before the administrative courts expect the latter to protect and safeguard them against actions on the part of the administrative authorities that they deem to be illegal or arbitrary by publishing the said courts to publish their rulings, so as to ensure that their behavior is impartial, transparent and governed by due process.

In this regard, there is a group of member States —i.e. Austria, Benin, Spain, Switzerland, Israel, Korea, Slovakia, Finland, France, Greece, Poland, Portugal Lithuania and Mexico— that publish anonymized public versions of their rulings on their websites, along with non-anonymized versions for the parties involved, omitting all data that enable people to identify litigants and third parties.

In the aforesaid legislations, the data omitted from public versions are those that enable people to identify the first and last names of the individuals named in the ruling, as well as any other identifying data and information that the different legislations may deem to be restricted or confidential.

Although there are no specific laws governing anonymization and data restriction in Germany, the Netherlands, Luxembourg and Turkey, the practice of the courts there is to anonymize personal data contained in the rulings that are disseminated via Internet.

Another group of countries publish their legal rulings with a certain degree of anonymization, omitting sensitive personal data — i.e. China, Canada, Australia, Hungary, Norway and Belgium, where such data are omitted in cases involving minors and certain victims in criminal cases. The Czech Republic, as a rule, publishes rulings, anonymizing names and other sensitive data except in cases where rulings are not published because they are internationally protected.

For its part, Colombia publishes such data without omissions on the website of its Council of State, notifying public entities about rulings in civil cases via an email system especially set up for that purpose.

Finally, there are countries such as Ivory Coast whose Administrative Divisions do not disseminate any data or rulings, while the Senegalese Supreme Court publishes rulings that are of particular interest on its internal website, with the decision to publish being taken, in principle, by the judges after issuing their rulings, so that the chief justices publish the chosen rulings via the Court's Documentation and Study Service, along with summaries of the said rulings for publication.

Question n°3 :

*Information-technology-based democracy: Does your country use computer tools in order to express the will of its people in elections, plebiscites, etc.? If so, how does it safeguard the security of such consultations?*

With regard to the use of computerized voting tools, some of the member countries of the International Association of Supreme Administrative Jurisdictions have implemented computerized voting systems in their elections, some use such systems only for plebiscites, and some continue to use traditional paper ballots

Poland, Portugal and Switzerland use computerized voting systems in their local-government elections, while France has been using computerized voting machines in some of its municipalities since March, 1973, and, in recent years, Mexico has allowed its citizens who live abroad to cast computerized votes.

Some countries have a mixed system, including Belgium, where, under a law passed on February 7<sup>th</sup>, 2014, computerized voting is allowed, but with paper-vote backups.

Germany, Austria, Greece, Hungary, Luxembourg, Slovakia, Thailand and Turkey do not have computerized voting systems, though they do use them for making policy proposals to their parliaments and carrying out plebiscites, while Korea permits the use of such systems for electing the members of some institutions and bodies approved by its National Electoral Commission.

Though Colombia has no computerized voting system, it has passed a law mandating that one be set up.

Another group of countries, including Finland and Holland, tried to set up computerized voting systems, but, due to their peculiar circumstances, decided to postpone their use and go back to using paper ballots.

For their part, Benin, the Czech Republic, Ivory Coast, Norway, Italy, Canada, Lithuania, Senegal and Sweden do not plan to use computerized voting systems, preferring traditional paper ballots.

## 1.2] Computerized tools and judging

### Question n°1 :

*Inherent features of teleworking: Can administrative judges engage in teleworking? If so, which computerized tools (specific applications, Internet portals, VPNs, etc.) are available to them for the purpose of examining files online?*

Thanks to the use of technologies and the improved security thereof, the new ways of working include the safe, reliable option of teleworking, which is an especially useful way of avoiding losing time in commuting, and of operating in emergencies such as the earthquake that hit Mexico in September of 2017, when people who were far from their workplaces were able to work from home.

Normally, the online platforms used by courts are accessible, via wireless Internet, to all users with a valid access certificate based on an Access Key and Password and, sometimes, a two-step, double-verification electronic-signature system consisting of a robust password followed by a corroborating text message. Judges in Germany, Australia, Austria, Belgium, Canada, Korea, Chile, France, Finland, Greece, the Netherlands, Portugal, Mexico, Norway, Italy, Israel and Turkey can consult computerized files from their homes, using their work or personal computers, so long as these duly registered in the domain, thus being able to look at files and other computerized documents, check precedents, perform general office tasks and carry out all the different stages of proceedings online, including issuing final rulings.

The only court in Spain that has computerized systems is the Audiencia Nacional (National High Court), whose judges are able to use all kinds of teleworking tools, including an Internet portal with computerized files, a VPN and an electronic signature, though the said country has created an It project aimed at making it possible for trial proceedings may be what is colloquially called “paper free”, being carried out digitally from beginning to end,

Judges in the Czech Republic and Sweden have remote access to databases using a safe Virtual Private Network (VPN), while Luxembourg, though such access is not forbidden there, still has no special platform that to afford it.

For its part, the Polish court system will have remote access to legal files and documents submitted by parties in trials as of May, 2019.

Thailand plans to implement the E-ADMINCOURT system, which will be open to the public and enable judges to engage in teleworking and consult precedents, as occurs in the Czech Republic, where computerized jurisdiction and computerized legal archives are being developed. Meanwhile, the courts in both Thailand and the Czech Republic are already teleworking via VPN links.

Finally, while Benin, Switzerland, Morocco, Colombia, Lithuania, Ivory Coast and Senegal have still not introduced teleworking, unlike Lithuania, Ivory Coast and Senegal, the first four of these — Benin, Switzerland, Morocco and Colombia — have already drawn up plans to do and even passed laws mandating it.

Question n°2 :

*Aspects relating to the professional use of computer tools: Which computer tools (search engines for consulting precedents, databases, support software for the drawing up of rulings, etc.) are available to support administrative judges in their work?*

In this regard, several of the member countries of the International Association of Supreme Administrative Jurisdictions have computer tools for consulting files, documents and precedents both internally, via Intranets, and also via paid access to private tools, and, in some cases, they have tools for drafting rulings and platforms that support them throughout the trial process.

As mentioned above, Germany, Australia, Austria, Germany, Canada, Korea, Chile, France, Finland, Greece, The Netherlands, Portugal, Mexico, Norway, Italy, Israel and Turkey have platforms that enable to consult case files, precedents and other digitized documents, and, in some cases, support them throughout the whole trial process, up to the issuance of the final ruling.

Thailand's Supreme Administrative Court has access to desktop and personal computers, and its judges have access to tablets. The ADMINCOURT system, which affords direct access to the said judges, and even enables them to draft rulings, is pending implementation in that country.

Spanish judges have several computer tools, as well as a webpage operated by their country's Judicial Branch Council (Consejo General del Poder Judicial), accessed via a security password, where precedents, laws and legal doctrine can be consulted.

Morocco has an online judicial-branch database, an online legal journal, a computerized database of legal files, and an online support system for drafting rulings.

Judges in the Czech Republic can access the databases of their country's Supreme Court, as well as its database of laws and precedents, to consult records, court rulings, laws and precedents.

The Colombian legal system has a series of resources that are crucial to its running, and is envisaging setting up an online justice system.

In Slovakia trials can be held using the "ASPI (Wolters Kluwer)" automated legal-information system, the "Beck Online" system, and the "Nextcloud" system to share files at the divisional level.

Polish judges have special computer programs for recording court orders and rulings, as well as a program for storing legal files.

The Swiss Federal Supreme Court has a case-law-search engine, as well as one for consulting articles and doctrines and one that enables users to check the status of files.

Legal files in Benin are stored in flat format so that legal institutions and their staff can consult them via online searches, paying a subscription to Internet operators, while Benin also has an Internet site for consulting precedents.

Another group of member countries states, for purposes of this Rapporteurship, that it only has databases for consulting precedents and doctrines. One such country is Lithuania, whose courts use the "Infolex" system, which consists of a private system for consulting precedents and court records, to which all lawyers can subscribe. The said system can be used by the country's administrative judges to consult anonymized rulings that have been published.

For their part, Luxembourg and Sweden have search systems and systems for consulting both national and European case law.

The Ivory Coast's Administrative Division has a case-law database called "COMOE" as well as a subscription to the "LexisNexis" public-law system and the online versions of the journals put out by the French publisher, Dalloz, AJDA (L'Actualité Juridique du Droit Administratif) and RFDA (Revue Française de Droit Administratif), while, as well as having subscriptions to the aforementioned journals, Senegal's Administrative Court has equipped its judges with both desktop and portable computers.

#### *Question n°3 :*

*Features relating to the professional use of computer tools: How is the security of online search and teleworking tools safeguarded?*

The member countries of the Association of Supreme Administrative Jurisdictions, have implemented systems to safeguard the security of their online search and teleworking tools that accord with the complexity of the said tools, which, as we have seen, range from advanced security programs that require the inputting of a user name and a password, along with an electronic signature, along with sophisticated antivirus systems, and Secure Socket Layer (SSL) protocols, web-surfing protocols, servers that allow the encryption and decryption of Internet-transmitted data and Transport Layer Security (TLS), in an updated, more secure SSL version, to ones that only need the standard security programs used in all computers, since they have no platforms.

One of the countries with high security norms is Turkey, whose National Legal Information System (Turkish acronym: UYAP), as already mentioned, requires users to be members of the Turkish Law Council and have electronic and cell-phone signatures, as well as requiring validation of both the user and the server and that the connection be encoded, and have an SSL protocol to ensure data-exchange security and antivirus software in the computers of judges and prosecutors.

In France, teleworking applications such as Ariane, Ariane Archives and the "Guide du Rapporteur" (Rapporteur's Guidebook) can only be accessed via the Council of State's Internet, access to which is protected and can only be afforded by means of a user code and a password.

In Mexico, the security of the systems of the Federal Tribunal of Administrative Justice is safeguarded by limiting access to users who are duly registered, who can only enter it by inputting a user name, a password and, where required, an electronic signature along with encrypted information.

The same applies for Germany, Portugal and Spain where access to the systems for teleworking and other purposes requires electronic-signature authentication.

In another group of countries, the courts use security-protection organizations. For example, in Finland the Government Information Technology and Communications Center (Finnish acronym: Valtori) provides the state-level bureaucracies with Testing, Inspection and Certification (TIC) services.

Likewise, in Austria such services are provided to the Supreme Administrative Tribunal by the Bundesrechenzentrum GmbH (BRZ GmbH) Federal Computer Centre, Ltd.), subject to the prior payment of a fee.

Other courts have special protocols. For example, the Australian Administrative Tribunal complies with the Procurator General's Protective Security Policy Framework (PSPF) in order to protect itself against all security risks and threats.

Most of the member countries' administrative courts have user-authentication security based on user names, passwords and antivirus programs, as is the case with Chile, Thailand, Canada, Korea, Norway and Morocco, which also require two-step user authentication for access to their platforms. Likewise, in Hungary those wishing to access the Supreme Court's remote desktop must input an encrypted VPN, after completing a two-step identification process, while entry to the courts' restricted-access and distance-access system only requires a user name and a password.

In Austria and Poland, legal records and files can only be consulted from desktop and portable computers that have permission to use the court-authorized information-technology services. For its part, Israel's system can only be accessed by using a smartcard or be means of the government's secure-identification service.

The Belgium tribunal's intranet can only be accessed by using a log-in code and a password, while entry to its external network is protected by aligning two firewalls.

The administrative courts in the Czech Republic have installed antivirus software in every desktop and portable computer, and teleworking is only possible if the Supreme Court applies to, and is permitted by, the Ministry of Justice, to engage in it, using a renewable digital-certificate card provided by the said Ministry.

In contrast, there is a group of jurisdictions that have not implemented any special security measures other than antivirus programs. Among these is Colombia, which is about to launch a teleworking platform, along with Lithuania and Ivory Coast, whose administrative courts only have basic web security, and have not adopted any special security measures.

The courts in Benin safeguard security by using antivirus programs, while security in Senegal is provided by the staff of the tribunal's IT-service department.

Question n°4 :

*Features relating to the professional use of IT tools: What disciplinary measures are taken when the teleworking tools provided by the jurisdiction are misused?*

With regard to such disciplinary measures, some of the member countries of the Association of Supreme Administrative Jurisdictions have special courts that impose sanctions for the misuse of IT tools, other member countries apply their general laws governing criminal and administrative responsibility in the case of civil servants, who misuse the said tools.

Employees of the Canadian Supreme Court are governed by the Information Technology Guidelines, which stipulate which uses of IT tools are acceptable, while employees of the Australian Administrative Court must comply with the latter's policy on the use and security of IT systems.

The supervisory departments of China's Supreme Administrative Court deal with IT security as part and parcel of general security and inspection, and investigate all infractions.

In the event that an Electronic File pertaining to an online trial held before Mexico's Federal Tribunal of Administrative Justice is altered, destroyed by an internal user, or that part of the information therein is lost by such a user, the said Tribunal files the pertinent charges in order to initiate an administrative-responsibility proceeding, reserving the right to take whatsoever other legal actions as it sees fit against the infringer.

The Austrian Civil Service Law, which governs government officials — other than federal judge s— along with employees of federal institutions, contains certain regulations on the use of IT and communications technology in the workplace.

Among the many jurisdictions that enforce general criminal-responsibility or administrative-responsibility laws in the event of illicit use of IT tools are Germany, Benin, Chile, the Czech Republic , Korea, Slovakia, Spain, Finland , France, Greece, Italy, Israel, Lithuania, Luxembourg, Norway, The Netherlands , Poland , Portugal, Senegal, Sweden Thailand and Turkey, which do not envisage specific sanctions for the improper use of their courts' IT tools measures, but, rather, apply general rules in cases where civil servants commit offences.

Switzerland, Ivory Coast and Colombia —which have no specific regulations governing the misuse of IT tools, which is currently governed by the existing criminal- and administrative-responsibility laws— are about to implement teleworking.





# /// TOPIC 2

## ELECTRONIC JURISDICTION

### 2.1] Electronic Jurisdiction (Online Administrative Litigation)

#### Question n°1 :

*Is your jurisdiction able to engage in teleworking. If so, which tasks (bringing suits, exchanging conclusions and evidence, holding trials, notifying rulings, etc.) can be carried out online?*

In this area, the member countries of the IASAJ are clearly tending to initiate, carry out and settle administrative-litigation procedures entirely online. In some cases, litigation is carried out both online and also on paper in traditional courtrooms, as occurs in Canada, China, Colombia, Spain, Hungary, Lithuania, Morocco, Norway, the Czech Republic, Germany, Australia, Austria, Benin, Slovenia, Finland, France, Greece, the Netherlands, Portugal, Sweden and Mexico.

The countries that have online administrative-case-management systems include Germany, China, Hungary, Israel, Norway, Switzerland, Thailand, Turkey, Australia, Austria, Chile, Korea, Finland, France, Italy, Portugal and Mexico.

Among other countries, Poland, Germany, Slovakia, Luxembourg and Senegal will soon be implementing online justice systems, which they are either planning or piloting at this time.

It bears pointing out that Canada, Slovenia, Greece, the Netherlands, Lithuania and the Czech Republic, which are among the countries whose legal systems and regulations envisage the use of IT technology electronic for the procurement of justice, are among the many countries where trial documents are submit, received, consulted and reproduced — and notifications and other communications carried out — via email, digital mailbox or even text-messaging.

Practices range from mandating the use of electronic media for litigation to nations making it optional; we can say that where such use is mandatory, as is the case in Spain, it is incumbent on specific groups of people such as lawyers and other legal advisers, rather than on laymen. One country whose legal systems still does not use IT resources, is Ivory Coast, where litigation is traditional and carried out in courtrooms.

*Question n°2 :*

*Evidence submitted via electronic media: What is the probatory value of evidence submitted via electronic media?*

One can observe a growing tendency, in the jurisdictions, to use evidence submitted online both in both the pretrial and trial stages of the litigation process.

Indeed, most of the jurisdictions deem evidence submitted online, and also other supporting items thus submitted, to be valid in all legal proceedings, including litigatory ones. It should be pointed out that, as a rule, the legal provisions governing such submissions have their roots in Common Law, though Switzerland, Benin, Korea and Slovenia have special laws that stipulate the manner in which evidence submitted online must be authenticated.

An outstanding issue, in the case of electronically submitted evidence, is its authenticity or authorship. In Germany, for evidence to be deemed valid and provided by a legitimate, duly authorized party, it suffices for it to be uploaded to a platform devoted to processing and following up on case files, or transmitted via a similar IT system established for that purpose, by a user thereof whose identity has been validated and authenticated, while Canada, Israel, Luxembourg, Norway, Turkey, Germany, Poland, Portugal, Senegal and Mexico also mandate the use of an electronic signature.

## **2.2] The security of online legal proceedings**

*Question n°1 :*

*Electronic case files: Does your jurisdiction's domestic legal system have a mechanism for checking electronic signatures against handwritten ones. If so, in which cases is this done?*

As a rule, in IASAJ member countries, electronic signatures must be checked against handwritten ones in order to be deemed valid.

Basically, the provisions governing electronic signatures include ones mandating the use of digital certificates issued by authorized organizations that confirm the authorship, integrity and uncorrupted status of digital data from the moment when they are transmitted up to the moment they are delivered, with optional encryption technology. Nevertheless, Ivory Coast, China, Israel and Sweden —and above all, Lithuania, whose laws stipulate that electronic signatures shall have the same validity as photocopied ones, and mandate that the original document must be exhibited —do not deem electronic signatures to have the same validity as handwritten ones, or do not accept such electronic signatures under certain circumstances. Likewise, Senegal does not accept electronic signatures in cases having to do with family issues, inheritances, and personal security.

Generally, all parties in litigations, and also judges, can use electronic signatures, but in Canada only parties of the second part may use them, while petitions and pleadings before the French Council of State do not require an electronic signatures. Only Spain allows electronic signatures at the National Court, as its procedures are fully electronic. While the German jurisdiction accepts both documents with electronic signatures and ones with photocopied signatures that are transmitted via channels that are permitted under law, Finland, though it has special laws governing the electronic signatures, does not currently allow their use, but is working to implement it.

*Question n°2 :*

*The security of electronic case files. If your jurisdiction carries out administrative litigation online, what controls does it employ to protect electronic case files?*

Among other things, the jurisdictions that have implemented platforms restrict access and consultation by users, forbid the installation of alien programs or applications in their official computers, block certain Internet addresses, such as those pertaining to unsafe social networks and sites and require the periodic updating of electronic signatures and passwords, the migration of information from work stations to safer storage media such as central servers, use firewalls to prevent information from being filtered, make secure copies of data transmitted via private networks, and provide training and awareness-raising sessions to their officials and other employees on IT activities and the associated risks.

More attention is paid to certain aspects of security such as system access, which should require at least two steps (e.g. user authentication, which might be supplemented by the use of special access codes for consulting documents, as occurs in Belgium. Since ensuring the inviolability of data is a constant concern, in Canada and Thailand, the integrity of files is safeguarded by converting them to formats that do not allow them to be edited and enable them to be stamped. China, Israel and Morocco use automated document management, risk controls, case follow-up, information encryption and on-screen auditing to support their efforts to protect data, while Switzerland uses distribution platforms, and, in Germany, Chile, Korea and France, information can be registered in the system and stored for set periods.

Sometimes value-added security options are available to parties that wish to verify the authenticity of the documents uploaded to the platform via Internet. In Korea, the latter may be checked against the original digital records kept by the court, while, in Spain, when doubts about their authenticity arise, the originals of documents, and even of digitized images, can be directly examined.

In Germany, Chile, China, Slovakia, Slovenia, France, Greece, Italy and Sweden, system security can also be safeguarded by using different types of private network that permit communication between judges, lawyers and courts.

Question n°3 :

*Electronic communication tools in trials: Are these reliable ways of informing private parties about litigation proceedings?*

When countries set up digital platforms, as a rule information can be both sent and received via the latter, whether by means of electronic-mailbox or email systems, or via text messaging appointments that form part of the said systems. In other situations, notification can only be carried out using a separate digital-transmission vehicle that is not an integral part of the platform.

While the use of electronic communications media is largely optional, it is obligatory for qualified experts such as parties' lawyers. Typical examples of countries where this is the case are Belgium, Spain, Mexico and China, where notifications are verified using the digital system or platform. Canada, which allows information to be sent by e-mail, continues to use paper records in parallel. Colombia permits the use of electronic mailboxes, while Spain obliges professionals representing parties in lawsuits to carry out notifications via email. Israel prioritizes security, not sending the communication together with the document, but, rather, transmitting it via a link that can be only be used to recover it after it has been authenticated.

Germany and Mexico have online-justice platforms that also use email systems for communications about litigation proceedings, while, in Austria, filing an appeal is also made via email. In Korea, notifications effected using the online system are deemed valid when the addressee consults them, so long as this occurs within a week of their transmission, after which period the notification is deemed to have been made by default. In Greece, the only rulings that can be electronically notified are those made by the State Law Council, while the Dutch jurisdiction prefers that notifications and related communications be uploaded to its system's electronic portal rather than being sent via email.

In Portugal, the IT support system used by the administrative and tax courts certifies the time and date of transmission, providing the user with copies of the documents that are sent bearing the time and date of remittance, and, in cases where the said documents cannot be received, generating a message to that effect. Senegal uses encrypted emails to transmit notifications by parties in litigation proceedings and, where peripheral storage devices are used, requires that the password be sent separately.

## 2.3] Criminal liability and the electronic media.

### Question n°1 :

*IT-related offenses: Do the offenses punishable under country's laws include that of "IT-related damages to the civil service"?*

Since an overall study of each jurisdiction's legal codes and administrative-justice systems reveals that they do not envisage specific penalties for the offense of IT-related damage to the civil service, in the said jurisdictions indemnification for such damages must be sought under the laws governing non-contractual civil liability.

The offenses deemed to constitute IT-related crimes are undue breaches of the confidentiality of information systems and off mechanism affording access thereto, along with manipulation, deterioration and alteration of the said platforms, compromising their security so as to commit fraud or obtain illicit funds, illegally use personal data, forgery of documents, and violation or modification of computer equipment.

Crimes relating to the communication of information include: divulgence of confidential or incitement to divulge such information, the unauthorized rendering of electronic-certification for electronic signatures, the unauthorized provision or use of encryption services, the improper procurement of information via false Internet links, and the forgery of websites and domains. Also punishable are the creation and running of IT equipment and application that enable the aforesaid offenses to be committed.

Countries worth mentioning in this regard are Colombia, Austria and Spain, which do, indeed, have laws that govern IT-related damages to their civil services or governments. Hungary has laws that severely penalize illegal access to files and breaches of the confidentiality thereof by civil servants. For its part, Morocco's laws envisage two types of offense: the illicit divulgence of information and unauthorized access to data-processing systems, including automatic ones.

Norwegian law punishes those who commit IT-related crimes that cause damages to the civil service, while Thailand has a special law that penalizes damages to data or information systems such as threaten public security, economic stability or infrastructure, or are against the public interest. Benin's legal system contains laws punishing all those persons, including juridical persons, who violate data security, or commit fraud using an IT system or electronic-communications network.

Chile imposes penal sanctions for various offenses against the civil service, including the destruction or malicious impairment an information system, improper access to, alteration or destruction of such a system, and the malicious dissemination of IT-system data. While the offenses punishable under French law do not include IT-related damages to the civil service, the said country's laws do impose heavier penalties on those damaging automatic personal-data-processing systems implemented by the State. The Greek Criminal Code provides that any person who improperly or abusively copies, exposes, uses, discloses or infringes upon information or computer programs constituting state, scientific or professional secrets, or secrets of a public or private sector company, shall be punished by imprisonment of at least 3 months.

Question n°2 :

*Illegal access to systems: How is access to systems used by the civil service regulated?*

As already mentioned, access to online administrative litigation systems is via individual and/or group permits, using passwords or authentications for certain operations, such as the use of authorized electronic signatures, access registration, and the use of data by users. When granting access, emphasis is placed on users' job profiles, so that the said users can only access the system to the extent that their positions require them to do so.

Top-level legal staff responsible for processing files and settling the disputes to which the said files pertain can freely access the system, while other people must satisfy certain additional requirements in order to do so. Often, these aspects are regulated by the internal provisions of the courts themselves regulations. In addition to the preventive measures against illegal access to information systems, operating at the different user levels, there are also globally accepted protections that apply to service requests, and to the design of the applications and technical instruments provided by the information technologies and the communications.

It bears pointing out that Portugal affords access to IT systems via computers located in its courts, providing a temporary access code that is valid for up to four hours upon prior registration of the interested party and confirmation of his/her identity. The same applies to those who can show that they have a valid legal in the matter at hand, who are also afforded access via the same computer for a maximum of ten hours. Senegal only permits consultation of its Supreme Court's database by the said court's staff, but the bulletin in which its rulings and other related information are published can be freely consulted. Finland affords access to other branches of its civil service, while those wishing to access to legal IT systems in Spain must have electronic certificates issued by the authorities of the justice system.

Question n°3 :

*Criminal sanctions for IT-related offenses. What penal sanctions are imposed on those who illegally access legal files, violating the confidentiality of the information contained therein or either deliberately or accidentally modifying their contents? Is any sanction envisaged for civil servants found guilty of IT-related offenses?*

The penalties imposed on those illegally consulting the information stored in an IT system, or violating the confidentiality thereof are fines, imprisonment, or suspension and confiscation of the instruments used by them when committing the offenses.

Belgium and Austria impose special penalties on civil servants who commit violations and those who damage crucial infrastructure (defined as installations or systems that are essential for maintaining vital social functions such as health, security, and economic and social welfare). In Canada, the same criminal sanctions as are envisaged for fraud or breach of trust are imposed on civil servants who use or misuse computer data without due authorization in the course of their work activities. In Colombia, Turkey, Benin and

Slovenia more severe sanctions are imposed on civil servants who commit IT-related offenses, and the said offenders are also suspended.

Spain also imposes heavier penalties on offenders whose behavior hampers the provision of government services and prejudices civil-service activities. As already mentioned, Hungary, Greece and Norway have special sanctions for offenses committed by civil servants which prejudice government activities. As well as being subject to fines and imprisonment, in Lithuania those who breach the security of computer systems are required to do social service.

While Luxembourg imposes no specific penalties on civil servants who commit IT-related offenses, it indicates that disciplinary measures can be taken against them. Thailand imposes special sanctions on civil servants and police officers either deliberately or accidentally violate the confidentiality and integrity of computer data. In order to impose criminal sanctions, in addition to the elements that typify criminal conduct — Slovakia also requires proof that the offender was aware that the access in question was unauthorized — i.e. proof of intention to commit a crime.

Finland is another country that imposes harsher penalties when meddling with an IT system jeopardizes the supply of electrical power, the provision of medical treatment, the ability of the armed forces to defend the nation, the administration of justice or any other function that is crucial to society. Its laws also envisage imposing criminal sanctions on those who divulge confidential information to which they are privy due the positions that they hold. Italy reports that its courts have imposed criminal penalties on civil servants for breaches of confidentiality, as do the Netherlands, which reports that civil servants, including judges and court officials, can be sanctioned for divulging or leaking confidential files to the public. In Portugal, civil servants who, in the performance of their duties, manipulate an IT system so as to create false documents or data are subject to harsher penalties.





# /// TOPIC 3

## ETHICS AND DATA PROTECTION

### *Question n°1 :*

*The anonymization of court rulings. What steps are taken to safeguard personal data that are included in court rulings?*

Among the countries that regulate and/or implement technology designed to safeguard personal data are France, Benin and Chile. Although France has an “open-data” policy, like Benin, it also protects the personal data of individuals and authorities involved in litigation proceedings. Chile has also implemented an IT system that can safeguard the confidentiality of legal proceedings, while Austria’s courts themselves anonymize both access data and personal data that are made available to the public.

Korea is flexible and does not anonymize the personal data of its civil servants, while Finland and Australia —take a similar position, considering that personal data may or may not be published depending on the circumstances— publish the personal data of the judges or supreme-court justices who issue rulings. Finland keeps such data confidential unless there are specific legal justifications for publishing them, while Australia opts to anonymize such data. The policy in Slovakia is to limit the divulgence of personal data, whether by legal edict or by means of administrative rulings, while Spain, as set forth in the Organic Law Governing the Judicial Branch, has adopted a policy of discretion solely vis-à-vis the personal data of natural persons, affording access to the whole text of the ruling or to parts thereof, and not anonymizing personal data in the case of offenses committed against its Exchequer or the European Union, of smuggling that harms the latter entities.

Mexico has specific laws governing transparency and Access to public information, under which public versions of the rulings issued by its Federal Tribunal of Administrative Justice must be drawn up, eliminating sensitive personal data that are contained in the email addresses of plaintiffs, but the names and positions of the heads of administrative authorities against which claims are filed must be mentioned. When the name of the division issuing the ruling is given in the public version of the ruling, the identity of the judge can be revealed, and the aforesaid public versions must include the name and handwritten signature of the civil servants being sued. Notifications carried out via the Tribunal’s Law Journal must only be made to the parties in the case, and must include the name of the division, the opinion of the justice in question, the name of the court clerk, and, where applicable, the name of the plaintiff.

Lithuania, Poland, Italy, Greece, the Netherlands, Thailand, Portugal, Sweden, Hungary, Israel, China, Morocco, the Czech Republic, Norway, Switzerland (except for so called notorious cases (i.e. those widely mentioned by the press) and Luxembourg all have the same position on not admitting the publication of personal data of individuals (though the Netherlands allows the anonymization of personal data pertaining to employees of administrative authorities and legal entities, with the exception of natural persons who have powers of attorney or are otherwise empowered).

Likewise, Switzerland, Italy, Sweden, Greece and the Netherlands publish the personal data of lawyers, prosecutors and defenders, and civil servants, while Hungary, Norway, the Czech Republic, China and Luxembourg only publish the data of civil servants, though it bears mentioning that Luxembourg jurisdiction systematically divulges its rulings on its website, while its Constitutional Tribunal and Court of Appeals also systematically publish their rulings in full. In Switzerland, Italy and Greece, it is possible to request that information be completely anonymized, though only Greece is in the process of acquiring technology for protecting personal data. For its part, Portugal ensures that documents are anonymized via its 'Organization and Computing Division'.

In Germany and Slovenia, personal data divulged to third parties are deemed to be confidential par excellence, with the exception of data pertaining to civil servants, which are published. Senegal, however, has no regulations mandating that personal data be kept confidential, and so such data are published at the discretion of its Supreme Court.

Belgium, Canada and Ivory Coast do not have laws mandating the anonymization of personal data, and, if a private part wants to have such data anonymized, s/he must expressly request that this be done. For its part, Colombia considers that parties should know who the judges hearing their cases will be so as to ensure a transparent, lawful trials.

#### *Question n°2 :*

*The use of social networks by judges – Can judges use social networks, and, if so, under what circumstances? Which regulations (i.e. laws, ethics codes, etc.) stipulate the circumstances under which judges can use social networks?*

In this regard, we can report that some countries do, indeed, have specific regulations that contain guidelines on the use of social networks; Benin has an IT-ethics code and Slovakia's Law Governing Judges and Counsellors states that the latter are forbidden to express their opinions about matters that are still sub judice or res judicata in proceedings that have still not been terminated, being obliged to ensure that their conduct is always honorable and ethical.

France also has an ethics code that contains several provisions regarding the use of social networks by judges, while Greece has a 'Code Governing the Organization of Tribunals' and a 'Judicial Branch Statute' that sets forth the basic duties of the members of that branch and authorizes judges to use social networks, but without contravening the stipulations of the said statute, as does Slovenia.

For its part, Chile has a proactive attitude about the use of social networks, which is recommended by its Supreme Court, while justices in Spain can use such networks, even when identifying themselves as such, on the grounds that free speech is a constitutional right, so long as they do not breach ethical principles.

Other countries where justices and judges can use social networks are Spain, Poland, Lithuania, Israel, Hungary, Colombia, Canada, Sweden, Senegal, Portugal, Belgium, Ivory

Coast, Morocco, the Czech Republic, Switzerland, Thailand and Austria, though, while it is true that the said countries have no specific regulations governing social-network use, it is also the case that, like the countries listed in the previous paragraph, while their judges can use such networks, even when identifying themselves as such, on the grounds that free speech is a constitutional right, they may not breach existing ethics codes and must ensure that their conduct is always honorable in keeping with the government positions that they hold.

While the Chinese and Belgian jurisdictions have an official document governing the use of social media, Norway and Thailand rely on ethics and 'good customs', except where the latter contravene the law, meriting disciplinary measures.

Germany and Australia limit their judges personal use of social networks, and also limit even further their use of such networks in their capacity of civil servants. For their part, the Netherlands, while not forbidding their judges to use social networks, do recommend that they refrain from using them or use them in a limited way. It bears adding that in Luxembourg, which still does not have any specific regulations forbidding social-network use, the Judicial Branch is currently urged to abide ethical principles when using such networks. Finally, judges in Spain, Finland and Italy are free to use social networks at will, and Spain even recommends their use.

Although Mexico's Federal Tribunal of Administrative Justice does not forbid the personal use of social networks by its justices and other officials, it does have internal guidelines that govern their use. Indubitably, social networks are not communications media capable of providing transparent responses to requests for government-held information (i.e. they are not effective means of providing updates on trial status, opinions issued by judges or court rulings).

### *Question n°3 :*

*The use of IT tools used to make, and respond to, complaints: Are IT tools used to make, and respond to, complaints about misconduct by judges? If so, how?*

The Czech Republic, Switzerland, Thailand, Turkey, Hungary, Israel, Lithuania, Luxembourg, Morocco, Norway, Ivory Coast, Spain, Sweden, Belgium, Canada, Portugal, Greece, Finland and France do not have IT tools that serve for the above purposes, but only email systems, while Spain only uses such tools for purposes of case-file control.

Among other countries, Chile permits the use of IT tools and has, indeed, has implemented such use, employing the said tools for disciplinary purposes — i.e. to investigate complaints about members of the Judicial Branch and respond to them. Likewise, Korea is using a Supreme-Court website for the same purposes, as well as an online ombudsman and an intranet to be used by the members of the said court to report any improper or unethical behavior.

Slovenia favors the use of IT tools, while Italy has a computer system capable of processing complex statistics and ensuring the timely issuance of rulings. The Netherlands and Colombia monitor the behavior and access to Internet sites of court officials, as well as the information that they receive and transmit. For its part, China is piloting a risk-control-and prevention system, an automatic monitoring system, and an evaluation system.

In Mexico, IT tools are only used for purposes of statistical control pertaining to proceedings that are underway; they are not used to make, or respond to, complaints about improper behavior by judges, though they may be so used in the future when the necessary conditions exist and pertinent guidelines exist, until which time all such complaints are made, and responded to, in writing.





**MINUTES OF THE  
COMMISSIONS WORK**

## REPORT BY THE IMPACT OF DIGITAL TECHNOLOGY ON THE WORK AND ORGANISATION OF ADMINISTRATIVE JURISDICTIONS COMMISSION

### Participants:

Australia, Belgium, Benin, China, Finland, Greece, Italy, Mozambique, Poland, Senegal, Switzerland, Thailand, Turkey.

### Chairperson:

Mr. Ousmane Batoko, *President of the Supreme court of Benin*

### Rapporteur:

Mr. Yunus Emre Yilmazoglu, *Senior rapporteur judge of the Council of State of the Republic of Turkey*

The first session was opened by Mr. Ousmane Batoko, from the Supreme Court of Benin as the Chair of Round Table one. After his opening remarks, Mr. He Xiao Rong from the Supreme People's Court of China took the floor for his presentation, in which he gave a detailed overview about China's electronic court proceedings, including several examples such as electronic filing of cases, submission of evidence related to files, video hearings, micro mobile court application for following proceeding remotely and case law search. He also mentioned the use of internet for strengthening transparency through publishing all activities taking place in the judiciary. Finally, he shared some important statistics about digitalization of Court proceedings in the People's Republic of China. After his presentation, Members of Round Table I started the discussion on the principle of *bis de eadem re ne sit actio*, which forbids the duplication of actions. Each Country made remarks about whether this principle is applied in their jurisdiction, and if applied, they gave information about the functioning of preliminary audit system. Afterwards, the country delegates discussed the topic of whose responsibility should it be to know that there were several cases filed. Is it the claimant or the judge given the electronic registry made available to him/her?

Delegates also discussed about consequences and sanctions of duplication of actions.

In this context, the representative of Slovenia raised the question of whether it is a right or an obligation for the judge to check whether several actions have been brought. He elaborated further that the IT tools are available to the judge, who can easily see if there were several actions. And, in the case of failure to do so, the case may arrive at the appeal instance to be solved. Based on this argument, the participants mentioned their country experiences on the use of IT tools and the benefits of it. It was understood that countries in Round Table I used IT tools for publishing court rulings on their websites, checking duplicated actions, searching for case law relevant to the action in front of them and following on the case law to ensure consistency and allow for communication among the Courts for the purpose of consistency. Next question of discussion was about whether it is possible or acceptable for a judge to use computer tools to search for rulings based on the parties' names, the amount sought and the judges' names etc.



The main concepts discussed in this framework include transparency, confidentiality and boundaries of confidentiality within each Country. It was underlined that the judge, with the tools available, can search for case law using the key words relevant to each search criterion.

A very important issue that arose during the discussions was the confidentiality of databases available, along with the publication of decisions, which is of relevance in this context. As required by the right to protection of private life, anonymization of court decisions and thus the protection of personal data were mentioned as essential requirements, which both have special significance in the case of vulnerable groups such as children, women and refugees. Anonymization of decisions can be done either automatically by the court or upon the request of parties. In administrative cases, where the state is the defendant, it may also be necessary to withhold the name of the public officer who took the act on behalf of the state in order to protect him/her. Discussions revealed that there are different country practices regarding the anonymization of judges. Some countries publish the name of the deciding judge as a Constitutional requirement, whereas in others importance is given to protection of the judge and his reputation (against severe criticism and threats) and for ensuring the functioning of judiciary.

In this regard, some representatives underlined that it is necessary to know the deciding Court and the judge along with any dissenting opinions, which led country representatives to discuss about the procedure of open hearings and cases for which hearings can be held behind close doors. Two examples were presented for the latter, the hearings in cases related to children and refugees. Tax disputes was another topic discussed in this context, and it was stated that the principle of open hearing is accepted as a general rule, while in some cases such as for protection of trade secrets, parties may request hearings behind close doors, which would then be decided by judge. In Slovenia, after amendment of the Law, it is required to write the names of Supreme Court judges who decided on the matter and how they decided, in civil and administrative judgments, which means those who voted in favour of the decision and those who opposed must be published. This may pose risks of safety and bring unpopularity on judges especially in tax cases costing governments thousands of euros.

Next question is question 3 related to parties' access to databases.

It is evident from the discussions that more databases should be available to Courts. As regards databases where court decisions are published, it was found out that some countries prepared public versions to be published in databases. It was underlined that parties' access to databases is essential within the framework of right to fair trial. After detailed discussions on who should be granted access to the system and which particular information should be available, it was agreed in conclusion that is important to make databases available to the public. However, in some cases to protect the parties and functioning of the judiciary some data can be withheld.

This was the end of the discussions about case study I.

On day 2 of the discussions, the second case study was addressed through discussions on methods of collecting public opinion and various forms of implementation.

Main points of discussion include the following:

- a) Should it be only for the private persons to cast vote in the method of referendum or should legal persons be allowed to vote?
- b) Measures to secure the voting procedure, such as prevention of voting several times.
- c) Legal consequences of acts against security of the voting procedure, such as annulment of the referendum and annulment of the Public Authority's decision based on the referendum.
- d) Who should be eligible for casting a vote? Reasons for any limitations?

It was agreed by the delegates that when an irregularity is found in a voluntary referendum, then the administrative court should question the legality of the authority's decision based on this referendum. Some countries stated that they don't have this method of collecting public opinion. Instead of this, they used the method of consultation or other methods in the case of environmental issues where people need to feed their opinion in.

As regards the possible consequence of annulment of the referendum, some country delegates stated that for annulment result of referendum must be absolutely impacted by the violation. As regards, eligibility for voting some country representatives stated opinions in favour of eligibility of legal persons to cast a vote, while others were against such eligibility. In the case of legal persons, it is the representative of the legal person casting a vote not the legal person itself. Therefore, the individual opinion of the representative may be reflected on the vote, which is one reason why legal persons should not be eligible. Some other representatives argued that if they have the interest, legal persons should be able to vote.

On the other hand, even if the referendum is voluntary it is an expression of people's will and for this reason procedural safeguards must be provided.

The second question led discussions to focus on the issue of security of the referendum. And it was agreed by the representatives that the referendum would be annulled after discovery of a system hacking to allow for several votes to be cast by one person. When procedural safeguards are not provided in the voting process, uncertainty occurs, which would render the result illegal.

Furthermore, difficulty of proving the act of manipulation in the voting was discussed, and it was underlined once again that voting is an important means for democratic expression and its security must be ensured.

Nevertheless, when an irregularity arises and the judge has to decide on it he should consider both the interest of plaintiff in challenging the referendum and the will of voters. The irregularity in this case would undermine the exercise of democratic rights and it is difficult to assess its impact, which would lead to annulment of the referendum.

Next item, question 3 was about which advice to give to authorities. Most judges agreed that it is not possible to give advice as a judge, while in some countries certain methods are available for the provision of such advice through various channels.

Country representatives who strictly avoided giving advice underlined the principle of separation of powers and added that if authorities sought for advice they could resort to other means such as hiring a lawyer, searching for case law, analysing related legal provisions etc.

And the main value to be protected should be independence of the Court as underlined by the representatives in the group. In countries where it is possible to ask for advice, the method used ensures that the opinion provided is not one of an individual judge but a collective opinion of the Court. In the case of France, for instance, when a new law or rule enters into force, giving advice can be useful for interpretation of the new law. However, if the court gets a case on this very matter, then it would be impossible to offer advice.

The discussions ended on this note for Commission 1.

Thank you for your attention.

**Yunus Emre YILMAZOGLU**

*Senior Rapporteur Judge of Plenary Sessions of the Tax Law Chamber  
of the Council of State of the Republic of Turkey*

## REPORT BY THE ELECTRONIC JURISDICTION AND ONLINE LITIGATION COMMISSION

### Participants:

Belgium, China, Colombia, France, Israel, Mexico, Mozambique, Netherlands, Portugal, Republic Of Korea, Thailand

### Chairperson:

Mr. Carlos Chaurand, *President of the Federal Tribunal of Administrative Justice of Mexico*

### Rapporteur:

Mr. Yves Gounin, *State Councillor, Delegate for International Relations of the Council of State of France.*

Our group included representatives of 11 institutions representing the five geographical groups that make up our Association: Europe, Africa, the Middle East, the Americas and Asia. Before answering the questions put to us, a methodological and semantic clarification was discussed on the subject of «e-jurisdiction». What is it all about? The term in fact refers to three related but distinct concepts. Only the first of these three concepts has been examined in the questions put to us. These are the electronic procedure, the electronic hearing and the arrangements under which a claimant may bring a case before the court using a paperless procedure; under which he may do so, where it is an option, under which he must do so, where it is an obligation.

Also within the scope of our study are the procedures for the exchange of pleadings between the claimant, the defendant and third parties involved, whether they are called upon to present the case or intervene on their own initiative. On the other hand, two other concepts, two other dimensions of electronic jurisdiction have not been taken into account, whether we welcome or deplore this. These are the electronic hearing, which consists, as an exception to the principle of a real, physical hearing involving judges and parties at a given time and in a given place, of derogating from this principle either by setting up video conferences or, radically, as is already the case in the United Kingdom with a fully electronic hearing (these are online dispute resolution). Finally, it is not within the scope of our study to consider the question of the electronic judge, the robot, the judge who can be assisted by artificial intelligence algorithms in order, firstly, to gather elements of case law, secondly, to draft a part, the most factual part of his judgment, or even, again whether we welcome it or are concerned about it, to help him propose reasoning leading to a solution. We shall therefore focus here on the procedure, or, as our Israeli colleague Yigal Mersel said, e-filing.

#### Four general remarks are in order.

**The first** is to note that whatever the level of development of our countries, we are all familiar with the implementation of dematerialised procedures, some countries being more advanced than others.

**Secondly**, in all countries this implementation has been gradual. Dematerialisation is not something that can be decreed, it is not something that can be done with a snap of the fingers, from one day to the next. It comes up against technical obstacles. It comes up against psychological obstacles. These psychological obstacles, moreover, do not come so much from the litigants, nor from the judges, as from the lawyers. Hence the implementation, often, of these procedures in the form of experimentation.

**The third** remark, linked to the previous one, is that the generalisation of these procedures is never absolute. This dematerialisation is obligatory for some, it is, and will remain, it has been said, optional for others. It is compulsory for those who are able to manage these instruments, to manipulate them. Firstly, public bodies. Secondly, parties with a lawyer. It is still optional, particularly for parties who do not have a lawyer, and in all the institutions represented in Commission No. 2 it remains so, even in South Korea, which gave us a particularly impressive, even intimidating, presentation of e-justice at the Venice Board meeting two years ago.

**The fourth** general remark, inspired by the French poet Alfred de Musset: «Never mind the bottle, as long as we get drunk», it doesn't matter whether the procedure is materialised, physical, paper or dematerialised, it is basically the same great principles, the same rules that must apply. The representatives of Colombia, Mr. Valbuena, and Mexico have invoked this point several times. The main principles of the adversarial process, of the administration of proof, continue to apply identically to dematerialised procedures. I quoted Musset; I could have quoted Giuseppe Tomasi di Lampedusa: «Everything must change so that everything remains the same».

After this lyrical impulse, which I hope you will have forgiven me for, I come much more prosaically to the examination of the questions that were put to us.

## CASE N°1

### The first question concerns the regime for documents submitted by an applicant in electronic form.

Let us put the question in context: as soon as electronics are installed, we are faced with exponential growth in the volume of applications. The multiplier factor of 10 was mentioned by the representative of the French Council of State, Ms Catherine Bergeal: an application is now 10 times larger than it used to be. This is quite understandable: whereas in the past, perhaps one party might have been reluctant to provide a hundred or so annexes because they had to be printed, slipped into an envelope, or stamped, today they can do so at the touch of a button, and they do not hesitate to do so. How should we react to this inflation? This is where the question of limiting the size of requests arises. Limitations that one could imagine in terms of the number of pages, or the number of characters, bytes, kilobytes or gigabytes. The measure makes sense and seems unavoidable to overcome this inflation, but it comes up against two obstacles.

The first is of a philosophical nature: is there not an infringement of the principle of free access to the judge which appears in many countries either in the Constitution or in a supra-national text.

Secondly, is it not a form of abstraction to set a limit that applies to all types of litigation? The President of the Council of State of Belgium, Mr Jacques Jaumotte, cited the case of the dossier on the award of a contract for a fighter aircraft which brought together, and, he said, this was quite normal and was not shocking, hundreds if not thousands of pieces. There would have been no sense in limiting ex ante the volume of that request.

More specifically, question No. 1 raised the following difficulty: what about a document submitted by a party that would be illegible because it was not in an electronic format that the court and the other parties could read? In fact, this is a false problem; it was answered, because in many countries the judge is not seized with an e-mail to which any kind of attachment in obscure electronic formats would be attached. The application is filed on a platform that only accepts attachments that are saved in the format that the platform can read.

Second difficulty, what about applications to which an indescribable mass of attachments would be sent in total disorder? Can it be required that these documents be indexed? What if they are not? Directly oppose inadmissibility? No. Most of the countries participating in Committee No. 2 are very pragmatic. The rule is as follows: an immediate inadmissibility is not opposed, but the applicant is asked to regularise his or her application by providing a duly referenced table of contents of the attached documents. Only if the applicant fails to respond to this formal notice will the application be declared inadmissible.

## Second question: how can the authenticity of the coins be guaranteed?

We had a debate on the meaning of this term. It is not a question of whether the documents provided are indeed authentic, but of whether it is really the person who claims to have filed them who has filed them. It is the question of the risk of identity theft, which, in the age of paper, was dealt with by the signature. The signature on a piece of paper attested to the identity of the person presenting it. What's wrong with electronic signatures? The answer could have been that the electronic signature, similar to the paper signature, made it possible to meet this challenge, but in fact, and this is very interesting, many countries do not use the electronic signature and consider that the identification of the applicant on the platform, thanks to his or her identifier and password, is sufficient to guarantee that he or she is indeed the one who has filed the application and the documents attached to it.

## Third question: how should electronic asymmetry be managed? What should be done if the claimant has filed documents via the internet and the defendant does not have access to the internet, in systems, which accept that the dematerialised procedure remains optional for certain parties?

I mentioned just now the pragmatism of the various courts of the Committee No. 2, and I should add here their compassion and sympathy for the third party who does not have Internet access, because in many countries the court registry takes charge of this asymmetry by means of two procedures:

- \* the first, mentioned in Portugal's reply, is to allow this applicant to come to the court to have access to a computer and consult the documents.
- \* the second, referred to in particular by Judge Ahn of South Korea, is to print out the application documents and send them to him by post free of charge. This is also the case in France.

This is case n°1.

## CASE N°2

Case No. 2 raised procedural issues that were a continuation of Case No. 1.

### **What happens if a party considers that documents filed by another party are inadmissible because they have not been signed?**

The answer to this question was already included in the answers mentioned above on the identification of the claimant's identity once the claimant is duly registered on the platform.

I will now move on to the next question, which concerns cases of technical accidents and malfunctions. What about a party who considers that it has not had access to electronic documents submitted by another party because there has been a breakdown, or because it has not been notified.

The answer is paradoxical and shows the astonishing superiority of electronics over paper. In the age of paper, it was not easy to prove that a party had had access to paper. With electronics, in today's brave new world, everything is easier, because the court, the host of the platform, has the electronic means to trace the actions of the various parties and to know whether, contrary to their allegations, they have had access to this or that piece of evidence.

So if there has been a breakdown, what should the judge's reaction be? It is the same as the one he had when, at the time of the paper, the plea alleging a breach of the adversarial principle was raised before him. The judge will assess the impact of this or that interruption of service, of which he is aware because he has the entire history of the connections between them, on the adversarial principle.

### **What happens if he rejects the argument and the party persists in its opposition and intends, after the judgment, either in the appeal it is going to file against the judgment handed down or in the liability claim it is going to file, to complain that the judge did not take into account a computer malfunction?**

Here again, the traditional rules of liability apply. As Mr Jacques Jaumotte, representative of Belgium, said, in a system of contractual liability, in the event of a malfunction in the public justice service, three elements must be present: fault, injury and a causal relationship between fault and injury.



**The last two questions, and I am decidedly much less concise than President Chaurand had been the day before yesterday, concern a hypothesis that we have all experienced in our lives: the one where suddenly, when we open our computer, a black screen appears.**

In these cases, you panic first, and then after 20 minutes of panic and irritation, you call the IT department. Usually a person who is the same age as our son or grandson arrives, without a tie and with a piece of chewing gum, and in 10 minutes he finds the document that had disappeared, and we are torn between two feelings: eternal gratitude and the shame of not having understood where the malfunction comes from. In the world of the 21st century, in the computer world indeed, it is miraculous, a document never quite disappears. There is always a duplicate somewhere, and several countries have intervened to highlight the efforts they have made to guarantee the security of their system. This sparked an interesting debate on the preservation of electronic data. It was a two-pronged debate.

The first was whether such information should not at some point be destroyed, whether its retention without any time limit violated national or supra-national regulations on the protection of personal data.

The second question we asked ourselves, symmetrical to the first, was how to preserve these documents on a long-term basis. This is the challenge of electronic archiving, and I am speaking before the former director of the Archives de France, who is now my superior and therefore I am cautious.

Finally, the question arises from a legal point of view. What happens if this electronic disappearance was the cause of a malicious act, committed for example by a registry officer? In this case, the principles of the criminal code apply, which is the case in France as in other countries. The penal code punishes the voluntary destruction of automated processing with fines or even imprisonment. Penalties are increased if the automated processing is carried out by the State and, in some countries, they are increased a second time if the perpetrator is a civil servant or an official vested with the prerogatives of public authority. These criminal sanctions must be combined with disciplinary sanctions: it is likely, if not certain, that the civil servant who has committed such embezzlement will be dismissed.



**In conclusion, I would like to stress two points. Our countries are at very different stages of development, have electronic infrastructures and more or less high levels of equipment, but they all share the same concern and have started the same process that of gradually introducing dematerialised procedures. We all apply common principles, the principle of pragmatism, first of all, and the concern to protect the rights of litigants. Electronics is not there to complicate things; it is there to simplify them.**

Thank you.

## REPORT BY THE ETHICS AND PROTECTION OF RIGHTS COMMISSION

### Participants:

France, Mexico, Thailand, Senegal, Spain, Chile, Italy, Ivory Coast, Switzerland, Colombia

### Chairperson:

Mrs Florence Aubry Girardin, *judge of the Federal tribunal of Switzerland*

### Rapporteur:

Mr. German Bula Escobar, *Member of the Council of state of Colombia*

The subject of the commission is open, because it addresses the deontological matter as a central issue. The sessions of the round table dealt with practical cases concerning judges' behavior, which were at the same time university professors. So, the distinction between the academic field and the jurisdictional scope was considered. And interesting topics were identified, which can be grouped as follows:

### **A] Common aspects between different countries when a judge acts in the academic field:**

1. It is accepted that judges teach at the university. And it is understood that there is freedom of teaching and expression. Universities also have their own codes of teaching conduct.
2. It is understood that teaching-judges can be critical about case law, in academic and legal terms.
3. In each case, the intention behind judicial decisions' disclosure or criticism can and must be distinguished in order to differentiate academic practice from other matters that may be censurable.
4. Disclosure of ongoing judicial cases is not allowed. The information that can be provided should refer to closed cases.
5. Pronouncements about ongoing cases can provoke judge's recusal.
6. There are data protection laws, which must be respected by teaching-judges.
7. Minors, issues that affect family life, victims of certain crimes and private matters on personal health are subject to protection to different extent and by different means.
8. The above considerations also apply to judges who write articles for academic magazines and journals.
9. There are recommendations that point out that in any case, whoever writes or gives an opinion orally, or in class, should make clear his or her judge status.

10. In relation to students participating in an internship, it was pointed out that they share the duty of protecting and not revealing information, just like a teaching-judge.

## **B] Common aspects between different countries with regard to the jurisdictional field:**

1. There are data protection laws, which must be respected by judges.
2. There are rapporteurship mechanisms to carry out the disclosure. According to the case and law of each country, these rapporteurships would be in charge of handling the information that is offered, and therefore of anonymizing it, if applicable and as appropriate.
3. Judgments are published on the web, as well as other information that contributes to transparency (calendar of judicial activity, etc.).
4. It is acknowledged the tensions between the need for transparency and publicity, on the one hand, and the obligation to protect information about people, on the other. It is recognized that publicity is implied due to procedural reasons and justice-users' rights. And, therefore, it is also recognized the existence of grey areas.
5. The practical difficulties of anonymization are also recognized.
6. Civil society organizations, as well as institutions from different branches of public power, usually demand information on judicial activity and on the judiciary, and follow up on conducts and case law positions.
7. The use of ICT and networks by the judiciary is not regulated; you only have to respect habeas data law. Problems concerning Information protection are recognized in online trials.
8. In any case, it is stressed the value of transparency as a pole of tension, and the importance of building trust and legitimacy for justice.
9. It is courts' common practice to have formal spokespersons, usually those who exercise the chairmanship of the institution.
10. Concerning the secrecy of judicial debates, it is recognized the importance of freedom of expression and changes of opinion of the judiciary, and how this generates tension in relation to the positive effect that publicity of judicial discussions could have with regard to citizens.
11. The common fundamentals of the liability arising from the failure to protect people information were reviewed, and it was recognized the need to derive that liability in each specific case, in order to distinguish between that of the judge and the one that would have those who make the dissemination by any means (particularly internet and social networks).

12. The need to advance in the clarification of the scope and concrete modes of information protection was acknowledged, inasmuch as there is a noticeable diversity of practices, regulations, and gray areas.
13. The crucial importance of the personal ethics of each member of the judiciary was emphasized, especially in times when new technologies imply the immediate and global dissemination of information.
14. The usage of a spokesperson by the courts helps to avoid the technological falsification of statements that can easily be attributed to judges today. Control is more complicated if court's voice is distributed.
15. The special nature of social networks was recognized, which allows the emergence of conflicts and debates in which the judiciary could get involved, and therefore it was acknowledge the need to exercise extreme caution regarding social networks' use. Any type of participation in trials that sometimes are attempted to carry out online should be avoided.
16. At the same time, it was recognized that ICTs and social networks can be useful and positive for judicial activity and to strengthen transparency and trust in judicial institutions.
17. It was stressed the importance of recognizing each judge as a bearer of citizens' rights, and the absence of judges whose life and opinions could be demanded as neutral for the purpose of being considered impartial at the time of taking jurisdictional decisions. Judicial decisions are made, according to the law and for the people; they are not personal decisions.
18. It was provided information about contemporary rights, coming from the law and case law, concerning habeas data, such as the update and elimination of information from databases and networks.

### **C] Other common considerations:**

1. In general, and under different modalities, it is considered improper to express negative opinions on fellowship's decisions. It is taken for granted fellowship duties. The decisions belong to the fellow.
2. Freedom of expression is taken for granted, but also, at the same time, the duty to respect the fellowship, as well as the duty to ensure trust in justice and its dignity.
3. In different forms -legal or disciplinary-, there are sanctions for judges that infringe upon justice dignity or act against the fellowship (in some countries it is expressly stated that judges last while their good behavior exists). For this purpose, in each country, there are institutions responsible for judging the corresponding cases (Deontological Colleges, Councils of the Judiciary, Ethical Courts, etc.).

4. In no case it is admissible for a judge to say or imply that the judgment he criticizes is mediated by corruption. In this case, all countries require specific complaints and the judge can be prosecuted for failing to report.
5. The role of the media was raised: disclosure only requires to respect habeas data law. It is known that the media can play and play a complex role concerning judicial proceedings and decisions.
6. In general terms, the need to review the relations of the judiciary with the media is recognized. The only substantial reform of the Bangalore Code of Conduct (2004) aims precisely at modernizing these relationships; but the matter admits further debate and elaboration.
7. Differences are recognized between the traditional disclosure of judgments and their physical consultation in the court secretariat, and the use of internet and social networks.
8. The importance of the debate on the opacity surrounding the management of big data was recognized.

## **D] Important differences to be highlighted**

1. Some countries (France, Spain) practice anonymization as a rule.
2. In some cases (France) anonymization extends even to moral persons. The dissociation also includes lawyers, law firms, and administrative officials whose acts or decisions are subject to legal review. It seeks to avoid leaving a trace of identification of the issues, with the purpose of protecting people.
3. A distinction is made between degrees of anonymization. In a deep degree, it is prohibited to offer data that allow to make correlations and identify, this way, the people involved.
4. In some countries there is a debate about dissociating the judge's name, considering the phenomenon of terrorism and the judicial branch officials' security and rights.
5. Although the concern is common, there are different treatments to the problem of judge's information, regarding protection against terrorism.
6. An annotation was made with regard to the capacity of criminality to have information about judges, details of the case, etc., beyond the state's control ability.
7. In some countries the anonymization of judge's autograph signature has also been proposed.
8. In most countries, the discussions presented during the highest courts' meetings are secret.

9. Some countries (Mexico -some are televised-, and Switzerland, in specific cases, and without television despite legislative pressures) hold public hearings in which, therefore, anonymization is not possible.
10. For most countries in the meeting, anonymization is exceptional.
11. In fact, a sentence is issued with complete information (except for information that is required to keep confidential by the law). And once it is issued, the hypothesis of being able to control its non-publicity beyond a certain point is not plausible.
12. In these, it is usual to distinguish between different confidential sources:
  - A. Ex officio -by judicial decision- (with support in the law).
  - B. At the request of a party (supported by the law).
  - C. Mandatory (people or situations specially protected by the law).
13. In most countries, it is usual to explain in writing a dissenting opinion, as well as the precision of nuances with respect to the *ratio decidendi* (by means of a concurring opinion).
14. The European Union has supranational regulations, but the conduct of its own courts is not homogeneous (Luxembourg, Strasbourg).
15. In some countries there is a debate: if administrative contentious decisions are about public sector, would there be anything to protect?
16. Some sectors of lawyers ask for anonymization.
17. In some countries (Thailand) citizens can report improper conduct through court's website.
18. In cases of special protection (minors), the matter goes beyond anonymization, until judgment's no publication.
19. In some countries (Mexico, Colombia), the Administration, when sending the administrative file to the judge, can demand or inform to the judiciary about the corresponding data protection.

## E] Deontology, moral, ethics and conscience

- ❖ Beyond as provided in law, ethics, conduct or deontology codes, the meeting highlighted the role of cultural practices that revolve around the concepts of deontology, moral, ethics and personal conscience of each judge.
- ❖ There is an obligation to refrain from public conduct that violates the values and dignity of justice.

- ❖ The deontological aspect is extracted from law, regulations, codes of conduct, codes of ethics and the like, and cultural practices.
- ❖ In general, it is clear that judges have high standards of conduct, given the fact that they cannot dissociate this condition of responsibility as judicial public officials, from that of ordinary citizens..
- ❖ Some countries reported that their judges are refractory to written ethical codes.
- ❖ In general, the crucial preventive role that peers play in the control of improper behavior (soft power) is recognized.
- ❖ While the theme of the commission is framed in the general issues of «Open Government» and «Open Justice», and taking into account that a good number of member countries of IASAJ are at the same time part of OGP - Open Government Partnership, the representative of Colombia proposed to study a concrete way of relationship between the two organizations that allows to advance in the studies and debates on these topics, with the highest possible quality..

**NOTE :**

After reading the previous report, concerns and interventions from the plenary session were heard, which allow adding the report as follows:

- In any case, it is recommended that judges and magistrates do not enter into controversies in social networks, or through the media.
- It is recommended to maintain and strengthen the good practice of using press releases, particularly in relation to complex issues, in order to communicate in a complete, clear and concise manner an adopted judicial decision.
- Special prudence is recommended in the use of restricted formats, in order to avoid that some expressions can be taken out of context and misused.
- It is emphasized the crucial importance and the irreplaceable role of the conscience of each judge, given the speed of the technical changes and its impact on information, communication and social networks.





3

**QUESTIONNAIRE**

# RAPPORTEURS

## /// PUBLIC LAW AND DIGITAL TECHNOLOGIES

### THEME 1 : IMPACT OF DIGITAL TECHNOLOGIES ON ADMINISTRATIVE JURISDICTIONS

#### [ SUJET 1 ] Digital environment in administrative matters

Question n°1 :

*Digital Identification. Does an accessible register of civil servants and attorneys exist? If so, how is it regulated? What is the extent of its regulation?*

Question n°2 :

*Transparency and access to information. What are the jurisdictions' obligations regarding the dissemination of its data and judgments (Open data)?*

Question n°3 :

*Digital Democracy. Does your country use electronic tools to allow the expression of popular will (elections, public consultations...)? If so, how is the use of such tools supervised and controlled by administrative judges? How is electronic consultations' security ensured?*

#### [ SUJET 2 ] Electronic tools and judges work

Question n°1 :

*Teleworking. Do administrative judges have the possibility of working remotely? If so, what are the digital and computer tools available to them (specific application, online portal, VPN ...) to process files remotely?*

Question n°2 :

*Professional use of digital tools. What types of digital tools are available to administrative judges to help them in their work (case law research tools, databases, judgment writing softwares, etc.)?*

Question n°3 :

*Professional use of digital tools. How is the security of computer tools for research and remote working ensured?*

Question n°4 :

*Professional use of computer tools. What are the possible disciplinary consequences of inappropriate use of digital work tools provided by the court?*

## THEME 2 : ELECTRONIC JURISDICTION

### [ SUJET 3 ] Electronic jurisdiction (Online administrative litigation)

Question n°1 :

*Does your jurisdiction have the possibility to deal with cases electronically? If so, what are the acts likely to be carried out digitally (referral of the jurisdiction, exchange of statements and written evidence, judgment, notification of the decision ...)?*

Question n°2 :

*Electronic evidence. What is their legal value?*

### [ SUJET 4 ] Dematerialized court proceedings security

Question n°1 :

*Digital jurisdictional record. Does your domestic legal system have a system designed to confer the same effects on electronic signatures as on handwritten signatures? If so, in which cases?*

Question n°2 :

*Digital jurisdictional record's security. In the case of dematerialized jurisdictional procedures, what measures are implemented in the handling of digital jurisdictional files to guarantee their security?*

Question n°3 :

*Electronic transmission of procedural documents. Is electronic transmission a reliable tool for the transmission of procedural acts to interested parties?*

### [ SUJET 5 ] Criminal liability and digital tools

Question n°1 :

*Computer Crimes. Is there in your internal legal system a tort of liability for computer damage to the public administration?*

Question n°2 :

*Illegal access to systems. How are the accesses to the systems used by the administrative jurisdiction regulated?*

Question n°3 :

*Criminal penalty of a computer crime. In the event of illegal access to court files with a breach of data confidentiality or an intentional or unintentional data modification, what are the criminal penalties provided for? Is there a specific sentence for public servants convicted of such offense?*

## THEME 3 : ETHICS AND PROTECTION OF RIGHTS

Question n°1 :

*Anonymization of court decisions. What measures are taken to ensure the confidentiality of personal data contained in court decisions? To what extent are court decisions anonymized (name of the judges, names of the clerks, name of the parties, other data likely to reveal the identity of the parties ...)?*

Question n°2 :

*Use of social networks by judges. Can judges use social networks and under which conditions? What are the rules overseeing it (law, code of ethics ...)?*

Question n°3 :

*Are digital tools used to control inappropriate actions of the judges or to complain about those inappropriate actions? How?*





# GENERAL REPORT

TECHNOLOGIES  
PUBLIC LAW AND THE NEW INFORMATION

2019