



SECTION III: ACCESS TO SCIENTIFIC KNOWLEDGE AND NEW TECHNOLOGIES

Lúcia da Luz Ribeiro, President of the Constitutional Court of Mozambique

Our presentation falls within the scope of the theme of this Session C, “Access to scientific knowledge and new technologies”.

The main objective is to present, in a systematic manner, the responses to the survey conducted on the aforementioned topic. The theme “*Access to scientific knowledge and new technologies*” is fundamental to the social, economic and intellectual progress of the peoples of our countries.

This importance is justified by the fact that science aims to understand and explain the world, whilst technology applies that knowledge to solve problems, transform society and create more efficient and innovative solutions, such as advances in various areas, notably health, education and productivity, and thus in the promotion of fundamental rights and their guarantee and defense through our constitutional courts.

Of the survey made available, 68 courts and equivalent institutions that are members of the World Conference on Constitutional Justice responded, out of a total of 124 members.

The survey consisted of 5 questions, set out as follows:

- (i) Is the right to digital connectivity (internet access) recognized in the relevant regulatory instruments of your country?
- (ii) – Are there adequate instruments in place to safeguard citizens’ right to receive information via social media, with guarantees of accuracy?
- (iii) Does your legal system have mechanisms to protect against the misuse of surveillance technologies, data





collection or other means of social control that may have indefinite effects? If so, what are these mechanisms?

(iv) Does your legal system have mechanisms to protect against the misuse of artificial intelligence systems that could threaten the full enjoyment of human rights by future generations? If so, what are these mechanisms?

(v) – Has your Court issued any relevant rulings on these matters? If so, could you briefly describe them?

The methodology we have adopted to best meet the stated objective is to analyze the common aspects of the responses provided for each question and, subsequently, to outline specific differences, followed by a brief evaluative summary.

QUESTION 1: *IS THE RIGHT TO DIGITAL CONNECTIVITY (INTERNET ACCESS) RECOGNISED IN THE RELEVANT REGULATORY INSTRUMENTS OF YOUR COUNTRY?*

a) Countries with a Constitution, specific legislation or a legal obligation regarding internet access

From the responses provided, it was found that 18 countries have specific legislation on internet access. Among these countries, a group stands out that has specific legislation, such as Finland (*Communications Market Act*), Japan, where almost 97% of households have broadband internet access, and Brazil (Law No. 12.965/2014 – “Marco Civil da Internet”) with nationwide coverage.

In Mozambican legal systems, the right to internet access is enshrined in the Constitution, through Articles 48 and 71 (Mozambique) and Articles 34 and 40 (Angola).





A distinguishing feature lies in the group of 35 countries that responded that the right to internet access is treated as forming part of the essential content of other fundamental rights and freedoms:

- This is the case in the European Union, where the recognition and protection of internet access is regarded as forming part of the essential content of the right to *freedom of expression, freedom of the press, access to information, etc.* This recognition is enshrined in EU Directive No. 2018/1972 of the European Parliament and the Council of Europe, of 11 December 2018. In this regard, there are judgments of the European Court of Human Rights that give concrete form to and enforce this right;
- b) Another distinguishing feature concerns federal states, where the right of access to the internet is guaranteed through regulations of the federal states rather than through federal legislation.

b) Cases concerning the legal treatment of the right to internet access

Several other countries, such as Slovenia, India and Turkey, have already issued rulings in their respective constitutional courts holding that *overt and arbitrary restrictions on the internet, including its shutdown*, violate rights. These rulings focus more on the limitations and restrictions on rights than on establishing positive obligations to provide connectivity.

However, judicial interpretations are made in accordance with each country's legislation.

There are, however, some countries that have telecommunications laws, universal service regulations or policies for service expansion, but often without a requirement for the state to guarantee minimum connectivity for all or for there to be clear legal remedies in the event of non-compliance.

In such situations, civil society has turned to the courts or regulatory actions to address restrictions on access or regulations that place an excessive burden on users.





This indicates that there is an understanding that limits on connectivity, high tariffs, or arbitrary disconnections may violate existing constitutional rights.

In the case of Mozambique, civil society took action (filing an injunction with a court in November 2024) demanding the immediate restoration of internet access following restrictions during the post-election period.

c) Countries with no reference

In this group of 15 countries, there is no legal or constitutional mention of internet access, digital connectivity or the role of information technologies as fundamental rights. In these contexts, the issue of connectivity appears only in economic policies or development strategies (e.g. Canada), and not as part of a legal framework for human rights.

There are four countries in the EU bloc that have only referred to the European framework (the European Electronic Communications Code).

QUESTION 2: ARE THERE ADEQUATE INSTRUMENTS TO SAFEGUARD CITIZENS' RIGHT TO RECEIVE INFORMATION VIA SOCIAL MEDIA, WITH GUARANTEES OF ACCURACY?

Generally speaking, of **the 124 member countries** of the World Conference on Constitutional Justice, **68 countries** responded to this question. It was possible to divide the responses into four groups:

1. Given that the advent of social media is relatively recent, we have a first group of countries—the largest—where this issue is enshrined in the Constitution, generally framed within the universal right to information and freedom of expression, namely **Armenia, Azerbaijan, Bulgaria, India, Iraq, Lithuania, and Armenia**, whose responses to this question are found solely in their respective Constitutions.

Also in this first group are countries that draw on both the Constitution and other national and/or EU laws, such as **Andorra, Denmark, Belarus, Belgium,**





Cambodia, Croatia, Cyprus, Finland, Germany, Hungary, Italy, Kazakhstan, Kyrgyzstan, Morocco, Mexico, Mongolia, Pakistan, Peru, Portugal, Spain and Mozambique .

In the specific case of Mozambique, this issue is addressed in the Constitution, through Article 71, concerning the use of information technology, in paragraphs 1, 2, 3 and 4, in conjunction with Law No. 34/2014 on Access to Information, the Penal Code and the Law on Combating Cybercrime.

2. In the second group of countries, this matter is governed by a specific law or a set of laws. Some (i) refer to a single law, as in the cases of , **Chad, Montenegro, Serbia, Turkey, Ethiopia, Moldova and Mali**; and (ii) others refer to various laws, namely **Algeria, Angola, Brazil, the Democratic Republic of the Congo, Indonesia, Ireland, Jordan, Kosovo, Liechtenstein, Madagascar, Mauritania and Mauritius.**
3. A third group of countries relies solely on European Union legislation to address this issue, namely , **Austria, the Czech Republic, the Netherlands and Slovakia.** However, this group also includes **France and Luxembourg,** where the response to this requirement stems from the interplay between European Union legislation and domestic provisions.
4. The fourth group comprises countries that categorically state they do not have adequate instruments for this purpose, such as **Albania, Burundi, Canada, Comoros, Costa Rica, Egypt, Bosnia and Herzegovina, Georgia, Israel, South Korea, Poland, Latvia, Macedonia, the Principality of Monaco, Namibia and Slovenia.**

In summary, of **the 68 countries** that responded to the survey, **52**, equivalent to **76.4%**, state that they have adequate instruments to safeguard citizens' right to receive information via social media, with guarantees of accuracy, whether through the Constitution, specific

legislation,





various laws or EU legislation, whilst the remaining 16, equivalent to 23.5%, do not have such instruments in place.

QUESTION 3: DOES YOUR LEGAL SYSTEM HAVE SAFEGUARDS AGAINST THE MISUSE OF SURVEILLANCE OR DATA COLLECTION TECHNOLOGIES OR OTHER MEANS OF SOCIAL CONTROL THAT MAY HAVE LASTING EFFECTS? IF SO, WHAT ARE THESE SAFEGUARDS?

The development of new information technologies that we are presented with on a daily basis and their increasing use in recent times, particularly Artificial Intelligence, calls for us to reflect on the following fundamental question: *are there legal mechanisms in place to address the impact of the misuse of surveillance technologies, ensuring that the right to privacy is upheld?*

Here is the table of responses to the survey on access to scientific knowledge and new technologies:

Member countries of the WCCJ (World Conference on Constitutional Justice)	124	100%
Total number of countries that responded to the questionnaire	69	55.6%
Countries that did not respond to the questionnaire	55	44.4%
Countries that responded on the basis of the Constitution	29	23.4%
Countries that responded on the basis of specific instruments	30	24.2%
Countries with no reference to a legal instrument	7	5.6%

From the table above, it can be seen that, out of a total of 124 member countries of the World Conference on Constitutional Justice, only 69 responded to the survey, representing 55.6%; 55 countries did not respond to the survey, representing 44.4%; 29 countries, accounting for 23.4%, find an answer to the question in question in the Constitution; 30 countries have specific instruments,



representing 24.2%; and seven (7) countries, accounting for 5.6%, make no reference to any legal instrument.

Andorra, Belgium, Croatia, amongst others, find a legal basis for addressing the above issue in the constitutional text, and in some cases also rely on other specific instruments, including institutions, to safeguard the right to privacy.

The Constitution of the Principality of Andorra, in Articles 14 and 15, guarantees fundamental rights, such as the right to privacy and intimacy. These rights provide a legal framework for challenging the misuse of surveillance technologies.

This country and several others in the European Union, whether through their constitutional text or via a specific instrument, find a legal basis for addressing this issue in the General Data Protection Regulation [*General Data Protection Regulation – (GDPR), adopted in 2016 and in force since 2018 – EU legislation governing how organizations handle the personal data of European Union residents*].

In other spheres, good examples can be cited, such as the experience of the Republic of Angola, which, in addition to adopting specific instruments to address this issue (*Law No. 22/11 of 17 June – the Personal Data Protection Act – and Act No. 2/20, of 22 January – the Video Surveillance Act, which regulates the implementation and operation of video surveillance systems, with strict rules to prevent excessive or unjustified monitoring: Limits on the Scope of Surveillance: Surveillance in private homes or inhabited buildings is strictly prohibited, unless expressly authorized by a court order or with the occupant's consent*), established the Data Protection Agency (ADP), which acts as the central authority for the inspection and supervision of entities responsible for the processing of personal data.

In Mozambique, there is still no single, comprehensive and fully operational law on the protection of personal data.





Regarding protection against the misuse of surveillance or data collection technologies or other means of social control that may have lasting effects, the current legal framework is grounded in the Constitution of the Republic, in paragraphs 1, 2, 3 and 4 of Article 71, which prohibit the use of computerized means for the recording and processing of individually identifiable data relating to political, philosophical or ideological beliefs, religious faith, party or trade union membership, and private life; of personal data contained in computerized records; access to archives, files and computerized records or databases to obtain personal data relating to third parties; the transfer of personal data from one computerized file to another belonging to different services or institutions, except in cases established by law or by court order.

There are other related instruments, such as the **Electronic Transactions Act (Law No. 3/2017 of 9 January)**, which sets out obligations for the processing of personal electronic data and requires that data collection clearly states the purposes and the identity of the data ‘processor’; **Regulation on the Registration and Licensing of Intermediary Providers of Electronic Services and Digital Platform Operators** (Decree 59/2023), a recent instrument regulating digital platforms and intermediary providers, imposing privacy and security responsibilities in data processing; **Cyber Security Policy and Strategy (Resolution No. 69/2021 of 31 December of the Council of Ministers)**, which is also part of the regulatory framework addressing cyber threats, which may include undue or abusive surveillance, although it is not specifically a surveillance law, the Right to Information Act (Act No. 34/2014), which establishes the right to information.

Currently under consideration is the draft Personal Data Protection Act. This draft aims to create a legal framework that safeguards citizens’ rights in the digital environment, promoting transparency and accountability among data processors.





The absence of protective mechanisms regulating the use of surveillance technologies, data collection or other means of social control that may have lasting effects, as is the case in countries such as Burundi, Comoros, the Democratic Republic of the Congo, Denmark, Latvia, Morocco and Peru, whether at the constitutional level or through specific instruments, creates a vacuum that allows for the commission of unimaginable acts that may infringe upon the privacy of personal data. It is therefore important to urge countries that do not have any legal instruments stipulating limits or restrictions on the use of surveillance technology to do so, in order to guarantee the security of citizens' personal data.

It is from this consideration that the urgent need arises to equip the constitutional text and/or legal instruments, given that, today, advanced technologies are proliferating as a global phenomenon; the regulatory instrument must be precise, dynamic and compatible with the nature of such surveillance technology, rigorously aligning the basis for the existence of specific laws that address the issue in question, in all its complexity, ensuring above all the protection of citizens' privacy. Furthermore, there is a need to be guided by mechanisms of strict penalties to discourage the misuse of surveillance technologies.

QUESTION 4: DOES YOUR LEGAL SYSTEM HAVE MECHANISMS TO PROTECT AGAINST THE MISUSE OF ARTIFICIAL INTELLIGENCE SYSTEMS THAT COULD THREATEN THE FULL ENJOYMENT OF HUMAN RIGHTS BY FUTURE GENERATIONS? IF SO, WHAT ARE THESE MECHANISMS?

Regarding the question above, it is important to note that, of the 65 countries that responded to the survey, a significant proportion do not have a specific legal framework that comprehensively addresses the regulation of artificial intelligence and its impact on human rights.





Consequently, in some legal systems, regulatory development is still at an early stage (examples include Angola, Mali and Mozambique), whilst in others, support is provided through a combination of various legal provisions, including the Data Protection Act; the Cybercrime Act; the Criminal Code; and fundamental rights enshrined in the constitution, such as the right to privacy, liberty, equality and freedom of expression.

Examples of this include: Algeria; Andorra; Angola; Armenia; Azerbaijan; Belarus; Brazil; Bulgaria; Canada; Slovenia; Egypt; Ethiopia; Georgia; Hungary; India; Indonesia; Israel; Jordan; the Republic of Korea; Kazakhstan; Kosovo; Kyrgyzstan; Madagascar; Mali; Mozambique; Mauritius; Mexico; Monaco; Mongolia; Montenegro; Pakistan; Peru; Serbia and Turkey. Therefore, 34 countries (52.3%).

Furthermore, countries such as Burundi; Cambodia; Chad; the Comoros; Costa Rica; Denmark; the Democratic Republic of the Congo; Iraq; Morocco; Mauritania; Moldova; Namibia and Suriname – that is, 13 countries (20%) – state that there are no mechanisms in their legal systems to protect against the misuse of artificial intelligence technology that threatens the full enjoyment of human rights by future generations.

On the other hand, some legal systems provide protection through a combination of existing data protection laws, human rights obligations and EU regulations (as they consider these to establish harmonized rules on artificial intelligence), as is the case in: Germany; Austria; Belgium; Cyprus; the Czech Republic; Croatia; Slovakia; Spain; Finland; France; Ireland; Italy; Liechtenstein; Lithuania; Luxembourg; the Netherlands; Poland; and Portugal. Therefore, 18 countries (27.6%).

In the case of Mozambique, although there is no legal framework specifically addressing matters related to safeguards against the misuse of artificial intelligence





systems that could threaten the full enjoyment of human rights by future generations, efforts are being made to establish institutional and regulatory mechanisms to mitigate the potential risks associated with the misuse of Artificial Intelligence (AI), particularly with regard to the long-term protection of fundamental rights, intergenerational equity and democratic values, namely:

- Resolution No. 69/2021, which approves the Cybersecurity Policy and Strategy for its Implementation;
- Draft Law establishing the legal framework and Cyber Security Strategy, which aims to respond effectively and efficiently to the challenges of the Information Society, as well as to ensure the security of citizens, institutions and the State, and the protection of information systems and critical infrastructure in cyberspace, in accordance with the provisions of Article 178(1) of the Constitution of the Republic.
- Draft Law establishing the legal framework for the protection of personal data, with a view to ensuring the security of personal data contained in physical and electronic records, the establishment and conditions of access to databases, and their use by public and private entities, taking into account the challenges posed by information and communication technologies, in accordance with national legislation and international best practice standards, pursuant to Article 178(1) of the Constitution of the Republic.

QUESTION 5: *HAS YOUR COURT ALREADY HANDED DOWN ANY RELEVANT JUDGMENTS ON THESE MATTERS? COULD YOU PLEASE DESCRIBE THEM BRIEFLY?*

a) Countries with relevant judgments issued

Regarding the central question, 21 countries, namely Portugal, Poland, Austria, Belarus, Belgium, Bulgaria, the Democratic Republic of the Congo, Egypt,





France, Germany, Spain, India, Indonesia, the Republic of Korea, Liechtenstein, Lithuania, Mauritius, Pakistan, Mexico, Slovenia and Turkey, have responded in the affirmative.

It can therefore be seen that various decisions have been issued relating to the use of artificial intelligence, technological surveillance, the right to information, freedom of expression in the digital sphere, internet restrictions, cybercrime, the right to personal data protection, the right to be forgotten, and the adaptation of the legal system to the digital reality, thereby ensuring, to a certain extent, the protection of human rights in the context of new technologies.

By way of example, the following decisions handed down by the courts may be cited: the recognition, for the first time, by the German Federal Constitutional Court in 1983 in the Census case (15 Dec –1 BvR 209/83 and others), of the fundamental right to informational self-determination, based on the general right of personality and human dignity.

In 2014, in the Twitter (Yaman Akdeniz and others) and YouTube (YouTube LLC) cases, the Turkish Constitutional Court ruled that blanket bans on access to these platforms violated freedom of expression, given that the legislation in force did not authorize the complete blocking of *websites*, but only of specific *URLs* by court order.

Furthermore, Spanish Constitutional Court Ruling 58/2018 of 4 June established pioneering case law regarding the right to be forgotten as an aspect of the right to data protection, which entails the deletion of such data when it is no longer necessary for the purposes for which it was processed. In this specific case, a media outlet was ordered to de-index from its search engine certain personal data of the applicant, which appeared in the newspaper's digital archive as a conviction for drug trafficking in a news article from the 1980s.





b) Countries with some reference

It appears that 16 countries, namely Andorra, Angola, Cyprus, the Czech Republic, Finland, Ireland, Israel, Italy, Kosovo, Luxembourg, Macedonia, Monaco, Mozambique, Slovenia, Canada and Hungary, gave a negative response to the central question; however, they acknowledge that the debate on the subject is evolving and that future legislation or judicial decisions may directly address the legal implications of Artificial Intelligence in areas such as data protection, privacy, internet access and surveillance.

Some highlighted the existence of relevant administrative decisions (such as in cases of data misuse or sanctions for the misuse of Artificial Intelligence by lawyers), whilst others cited constitutional rulings, such as the inadmissibility of telecommunications data in criminal proceedings or the suspension of internet access in times of crisis, as well as experience in the protection of personal data and various judicial decisions relating to internet access, privacy and data protection.

3. Countries not mentioned

It is worth noting that 26 countries, namely Albania, Algeria, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Brazil, Burundi, Chad, Cambodia, Comoros, Costa Rica, Croatia, Ethiopia, Kazakhstan, Kyrgyzstan, Latvia, Madagascar, Mali, Mauritania, Moldova, Mongolia, Montenegro, the Netherlands, Serbia and Suriname, merely gave a negative response to the central question.

FINAL CONSIDERATIONS

The responses provided by the Constitutional Courts to the questions on the theme of *“Access to scientific knowledge and new technologies”* have made it possible to assess the levels of progress and development of this category of fundamental rights,





particularly those emerging in the present day, with a focus on Artificial Intelligence.

Each country's level of economic and social development determines the extent of access to knowledge and new technologies, as well as the promotion of improvements in this technological environment through regulation and the intervention of constitutional courts to ensure the full exercise of this right.

It is clear that countries are still in the early stages of regulating Artificial Intelligence, a technology that increases the risk of fundamental rights being compromised, as Artificial Intelligence applications are capable of creating content and performing tasks that normally require human intelligence, such as learning, reasoning, problem-solving and recognition.

Therefore, the regulation of Artificial Intelligence and the scientific enhancement of Constitutional Courts to deal with this new technology constitute a fundamental part of current global challenges: that is to say, legislation and Constitutional Courts must not be an obstacle to technological development and innovation, yet at the same time, they must be capable of preventing the risk of fraud, cyber security breaches, violations of privacy and other fundamental rights of citizens.

Thank you very much for your attention.

Khanimambo!

