COMMITTEE: ITU - Human Rights

ISSUE: To what extent can States and international organizations establish common standards to protect human rights in the digital space against mass surveillance, facial recognition technologies, and censorship while balancing freedom of expression and national security?

CHAIRS: Yasen GOSPODINOV, Charlotte DAUCHEZ and Lois GARCIA

PRESENTATION OF THE CHAIR



Hello, everyone! My name is Charlotte Dauchez, and I'm 17 years old. At FerMUN 2027, I will have the great honor of serving as your co-chair on the Human Rights Committee. I'm a senior at the Ferney Voltaire International High School and have been part of FerMUN for two years, where I've served as a delegate and then as a committee chair. In my free time, I really enjoy playing badminton, playing the piano and guitar, and meeting new people.

At FerMUN 2027, I will co-chair the Human Rights Committee alongside Yasen and Lois. The issues we will address will focus on two topics that are becoming increasingly important in our society every day: refugee rights and access to technology, as well as the protection of human rights in the digital space.

Today, the internet offers numerous opportunities for freedom of expression and access to information, but it also creates new challenges for governments and international organizations. Technologies such as facial recognition, mass surveillance, and artificial intelligence can contribute to user safety. However, they can also infringe upon fundamental rights, including the right to privacy, freedom of expression, freedom of association, and access to information.

So I'm really looking forward to sharing the discussions on these topics with you. I wish you all the best in your preparations, and see you soon!

KEY WORDS

Human Rights: According to the United Nations, human rights are the inalienable rights of all human beings, regardless of race, sex, nationality, origin, language, religion, or any other status. They include, in particular, the right to life and liberty, as well as freedom of opinion and expression, and the right to work and education. Everyone must be able to exercise these rights equally and without discrimination.

Human Rights in the Digital Domain: The enforcement and protection of existing human rights in digital and online environments.

Biometric Data: Personal information relating to physical or biological characteristics, such as facial features, fingerprints, or iris patterns.

Data Protection: The protection of individuals' personal data and oversight of how that data is collected, processed, stored, and shared.

Censorship: Censorship is the restriction or even suppression of freedom of expression imposed by a higher authority (governmental, religious, or private) on books, media, or various forms of art accessible to the public.

Mass surveillance: Mass surveillance refers to the collection by a government of data on an entire population, rather than just on suspected individuals. Phone calls, messages, internet searches, and movements—everything can be recorded, often without citizens' knowledge.

Freedom of expression: a fundamental right that allows everyone to freely express their opinions, ideas, and beliefs through any means (speech, writing, images), without fear of reprisal from public authorities.

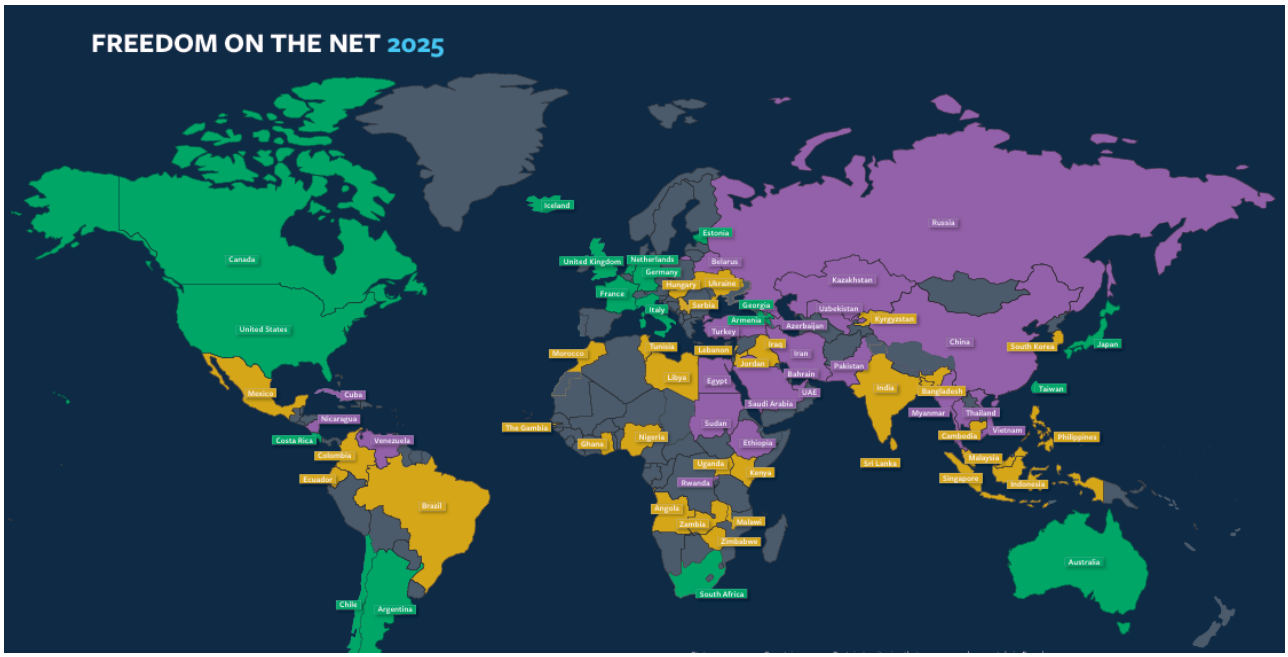
Freedom of the press: Freedom of the press is a fundamental right that guarantees everyone the right to report, investigate, and disseminate opinions without being subject to censorship or political or economic pressure.

OVERVIEW

Introduction

The digital realm has become essential to our societies, but it also presents a new arena of tension between security, innovation, and the protection of human rights. Freedom of expression, access to information, and privacy can be affected by the way governments and companies use digital technologies.

The map below, taken from Freedom House's *Freedom on the Net 2025* report, illustrates differences in internet freedom around the world. It serves as an introduction to the key issues examined in this context: surveillance, facial recognition, data protection, censorship, and freedom of expression.



: Free (18) : Partly free(32) : Not free (22) : Not assessed

Source: *Freedom on the Net 2025*

1)Facial recognition

Facial recognition is increasingly used by law enforcement and at border crossings to verify identity or ensure security. While it may have legitimate uses, its widespread adoption raises privacy concerns and risks turning public spaces into areas of constant surveillance.

The threat of algorithmic bias and false identifications:

Facial recognition systems are not infallible. Numerous studies show that machine learning algorithms have significantly higher error rates for women and ethnic minorities due to biases in the training data, which can lead to arbitrary arrests and reinforce discrimination.

For example, in the United States, several facial recognition misidentifications have led to the unjustified arrest of African American citizens (notably the Robert Williams case in Michigan in 2020), illustrating the concrete risks of algorithmic bias.

Group	**Taux d'erreur maximal**
Men with fair skin	0,8%
Women with dark skin	up to 34,7%

Source: J. Buolamwini et T. Gebru, « Gender Shades », MIT Media Lab, 2018 (gender classification errors*)*.

The legal framework: the european union's response:

The European Union has set a historic precedent with the AI Act (Regulation on AI), which in principle prohibits the use of remote, real-time facial recognition in public spaces by law enforcement agencies, except in very strictly defined exceptional cases (imminent terrorist threat, search for victims of serious crimes) and subject to prior judicial authorization. However, this level of regulation remains rare on other continents, such as in Asia or North America, where commercial and law enforcement uses are much less restrictive.

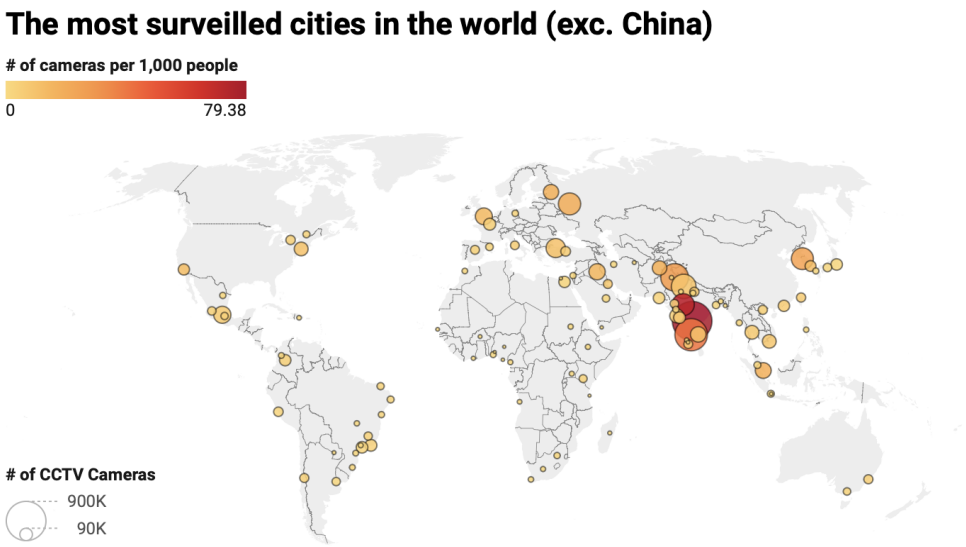
2) Mass surveillance

Large-scale

In 2013, Edward Snowden, a former employee of a US intelligence agency (the NSA), revealed that the United States and the United Kingdom were collecting the communications of millions of people around the world. Since then, the phenomenon has expanded with artificial intelligence, which can automatically analyse huge amounts of data. According to the Carnegie Endowment, an American research centre, at least 75 out of 176 countries already use AI to

monitor their populations. This is not limited to dictatorships: more than half of advanced democracies do it too. (Global map of AI surveillance, Carnegie)

Surveillance cameras clearly illustrate this trend. Comparitech estimates that there are more than 700 million public cameras worldwide, an average of 5.82 cameras per 1,000 people. The gaps are huge: Hyderabad has around 79 cameras per 1,000 people, while London ranks 12th with 13.4 per 1,000 people.

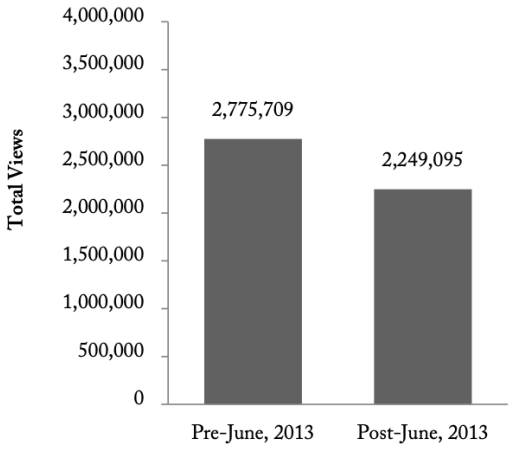


Source: Comparitech, *Surveillance camera statistics: which are the most surveilled cities*

(To make the map easier to read, data for China has been removed, but it is available on the website.)

A major international example is the case of *Big Brother Watch and Others v. the United Kingdom*, brought by the British NGO Big Brother Watch together with other organisations and journalists. In 2021, the European Court of Human Rights found violations of the right to respect for private life, due to the lack of independent authorisation and sufficient safeguards in the UK's bulk interception regime. It also found violations of freedom of expression linked to bulk interception and to the regimes for collecting communications data. However, the Court did not rule that bulk interception was unlawful in itself, provided it is strictly regulated.

Surveillance doesn't just infringe on privacy. It also leads citizens to self-censor: when people know they're being watched, they avoid certain topics. Following Snowden's revelations,



Average Monthly View Counts, Pre and Post June 2013. The reduction after the June 2013 surveillance revelations may suggest a chilling effect.

internet users significantly reduced their visits to Wikipedia pages on sensitive topics, such as terrorism.

Drop in Wikipedia visits after June 2013, Penney

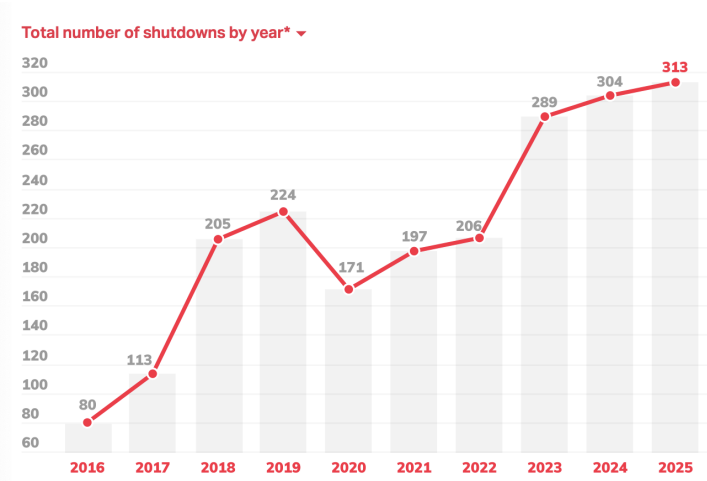
Source : Jon Penney, « Chilling Effects: Online Surveillance and Wikipedia Use », *Berkeley Technology Law Journal*, vol. 31, n° 1, 2016, p. 117 à 182.

In some countries, it can also lead to imprisonment. According to Freedom House, in at least 57 of the 72 countries studied, people have been arrested for their online posts.

3) Censorship and freedom of expression

The Internet has become an essential platform for political debate, journalism, education, and social interaction. Government restrictions on online content can therefore have a direct impact on freedom of expression and access to information.

Censorship tactics used by Governments: Shutting down the internet:

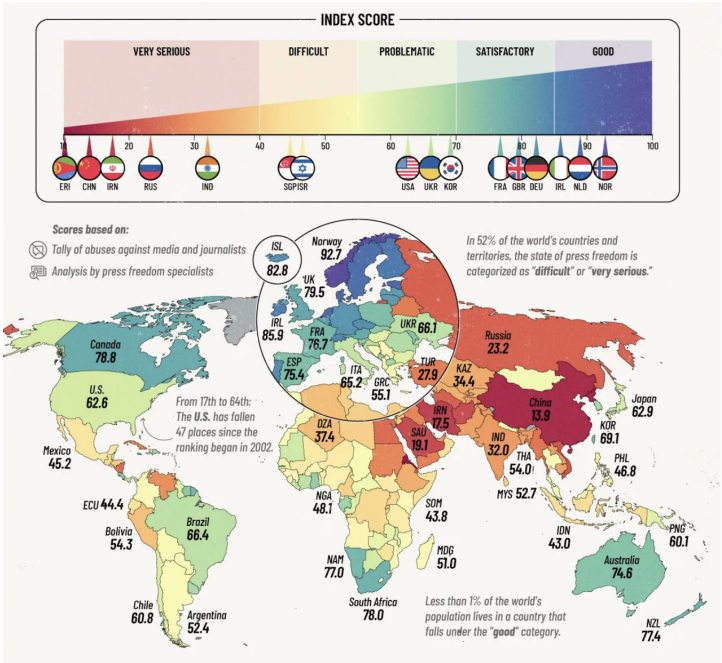


Some governments simply shut down the internet, either in a specific region or throughout the entire country. In 2025, the NGO Access Now documented 313 internet shutdowns in 52 countries—a record high. That's four times as many as in 2016. Myanmar tops the list with at least 95 shutdowns. India imposed 65, the highest number for a democracy.

Source : Access Now et coalition #KeepItOn, *Rising repression meets global resistance: Internet shutdowns in 2025*, mars 2026.

These blackouts occur mainly during wars, elections, or protests. Conflicts have caused 125 of them. They prevent people from staying informed and sometimes conceal serious human rights violations. They also have an economic cost: nearly $20 billion in losses worldwide in 2025.

Block and Punish:



Governments are also blocking social media platforms: in 2025, Facebook was blocked 31 times in 18 countries, and WhatsApp 27 times in 13 countries.

Journalists are particularly targeted. According to Reporters Without Borders, more than half of the world's countries are now in a "difficult" or "very serious" situation regarding press freedom. National security laws are increasingly being used against them

Carte de la liberté de la presse

Source: Visual Capitalist, d'après RSF

When can freedom of speech be restricted?

Freedom of expression is not absolute. International law, particularly Article 19 of the International Covenant on Civil and Political Rights (ICCPR), permits restrictions. However, these restrictions must meet three conditions:

1. they must be provided for by law;
2. they must pursue a legitimate purpose, such as national security, public order, or the protection of the rights of others;
3. they must be necessary and proportionate.

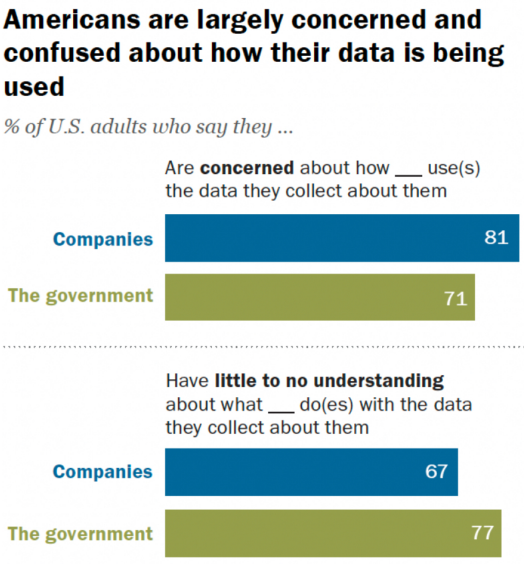
The problem is that the concept of national security remains vague. Many governments invoke it to justify censorship that is primarily intended to silence opponents. The challenge for the international community, therefore, is to better define these limits and to ensure that their application is overseen by independent judges rather than by the governments themselves.

4)Striking a balance between human rights and national security

Governments have legitimate reasons to monitor or restrict certain content: to prevent terrorist attacks, fight crime, or protect children. But too much security can stifle freedoms. The key question is where to draw the line.

Does more surveillance mean better protection?

Mass surveillance is not necessarily more effective than targeted surveillance. In the United States, an official oversight body, the PCLOB, examined the NSA's program in 2014 that collected phone records from nearly all Americans. It found no instances where the program had made a real difference in a counterterrorism investigation. The government, however, claimed that its programs had helped foil 54 plots. In reality, only 12 of those cases involved this program.



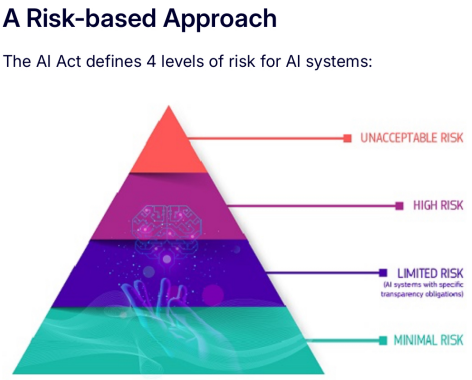
Public trust is also declining. Today, 71% of Americans say they are concerned about how the U.S. government uses their data, compared with 64% in 2019

Graph: Americans' concerns about the government's use of their data

Source: Pew research center, *Key findings about Americans and data privacy*, octobre 2023

Examples of balance:

The European Union is proposing a model through the AI Act. It classifies uses of AI according to their level of risk. Real-time facial recognition by law enforcement in public spaces is prohibited. There are three exceptions: searching for victims, preventing an imminent terrorist threat, or identifying a suspect in a serious crime. These exceptions have been criticized: some consider them too broad, and the analysis of images after the fact remains permitted.



Source: European commission, AI Act

Other safeguards are frequently mentioned: prior authorization from an independent judge, ex post review (as required by the Big Brother Watch ruling), and transparency regarding data requests made to companies

The challenge of global standards:

The United Nations Convention against Cybercrime clearly illustrates the difficulty. Proposed by Russia in 2017, it was adopted by the General Assembly in December 2024. It is the first universal framework for investigating crimes committed online. The Convention was opened for signature in Hanoi on October 25 and 26, 2025: 71 states and the European Union signed it during that ceremony. It remains open for signature until December 31, 2026, and has not yet entered into force.



Photo: Signing ceremony for the Convention in Hanoi, October 2025.
Source : ONU Info, *Sixty-five nations sign first UN treaty to fight cybercrime*, octobre 2025

But this convention continues to face heavy criticism. Its definition of cybercrime is vague, and each country remains free to decide how to protect human rights. A coalition of technology companies, including Meta and Microsoft, has even called it a “surveillance treaty.”

5) Conclusion

Facial recognition, mass surveillance, and censorship illustrate the complex relationship between digital technologies, human rights, freedom of expression, privacy, and national security.

Existing international and regional frameworks show that common standards are possible. The United Nations has established principles regarding privacy in the digital age, UNESCO has developed guidelines for the governance of digital platforms, and the European Union has put in place detailed rules regarding artificial intelligence and biometric identification.

However, these frameworks also show that international standards do not necessarily have to take the form of identical laws in every country. A more realistic approach might involve establishing minimum international safeguards based on legality, necessity, proportionality, transparency, independent oversight, and accountability.

For the delegates, the central issue is therefore not whether national security or human rights should take absolute priority, but rather how international standards can ensure that legitimate security measures remain compatible with fundamental rights.

RELEVANT TREATIES AND EVENTS

2021 — Council of Europe: Guidelines on Facial Recognition Provide recommendations to regulate the use of facial recognition and limit its risks to fundamental rights and personal data.

2023 — UN Human Rights Council Resolution A/HRC/RES/54/21: "The Right to Privacy in the Digital Age"

Demonstrates that the protection of privacy in the face of new technologies remains a topic of international concern.

2023 — UNESCO: Principles for the Governance of Digital Platforms

Propose a common framework to protect freedom of expression and access to information while combating harmful online content.

2024 — European Union: AI Act (EU Regulation 2024/1689)

Establishes common rules on artificial intelligence and, in particular, regulates remote biometric recognition, with strictly defined prohibitions and exceptions.

September 28 — International Day for Universal Access to Information

Proclaimed by the UN General Assembly in 2019, it highlights the link between access to information and freedom of expression.

POSSIBLES SOLUTIONS

1) Establish minimum international standards

The United Nations and other international organizations could develop common principles governing facial recognition, surveillance, biometric data, and online censorship. These standards could establish minimum safeguards while leaving it up to individual countries to decide how to implement them at the national level.

UNESCO already provides an example of this approach. Its Principles for the Governance of Digital Platforms were developed following consultations that yielded more than 10,000 contributions from 134 countries. In particular, they seek to safeguard freedom of expression and access to information while strengthening transparency and accountability on the part of platforms.

2) Strengthen independent oversight

Even if laws are in place, governments could therefore strengthen mechanisms for independent oversight of surveillance technologies. Courts, data protection authorities, independent regulators, parliamentary committees, or national human rights institutions could be tasked with reviewing the use of these technologies.



Independent oversight can help ensure that powers related to national security remain subject to legal safeguards.

Such oversight could also take the form of regular audits. For example, an independent authority could verify whether a facial recognition system is used only in situations provided for by law, whether data is properly protected, and whether the individuals concerned are not subject to unjustified discrimination.

3) Require legal authorization

Governments could establish clear legal frameworks before deploying intrusive digital technologies.

The laws could specify:

- Which technologies may be used.
- For what purposes they may be used.

- Which authorities are authorized to use them.
- How long the information may be retained.
- What safeguards must be in place.

The European Union's AI Act is an example of this approach. Under this regulation, certain uses of real-time remote biometric identification in public spaces for law enforcement purposes are prohibited, except under strictly defined circumstances. Exceptions to this prohibition require safeguards and prior authorization from an independent judicial or administrative authority.

4) Protect biometric data

Biometric data, such as fingerprints or facial images, require special protection: unlike a password, they cannot be changed if stolen. Governments could limit their collection to cases where it is necessary and proportionate, specify their intended use, and strictly regulate their storage, sharing, and retention periods. The European Union is already moving in this direction: the AI Act prohibits the creation of facial databases using images collected at random from the internet. The Office of the United Nations High Commissioner for Human Rights also points out that facial recognition can infringe on privacy and other fundamental rights when used without sufficient safeguards.

5) Increase transparency

Citizens cannot challenge surveillance or censorship if they are unaware that it exists. Governments could therefore publish more information about their surveillance practices, while protecting data that is truly sensitive to national security. In India, for example, orders to shut down the internet must already be made public. Technology companies could also publish government requests for access to data or for the removal of content. Google, Meta, and Microsoft already do this in their transparency reports. UNESCO's guidelines also emphasize the importance of transparency, accountability, and independent oversight to protect human rights online. These practices could become an international standard.

QUESTIONS TO CONSIDER

1. Does your country have laws governing communications surveillance? Who can authorize it?
2. Does your country use facial recognition? In what situations (police, borders, public spaces)?
3. Has your government ever shut down the internet or blocked social media platforms? For what reasons?
4. Has your country been involved in a spyware scandal, such as the Pegasus case?
5. Is there an independent body in your country that oversees intelligence agencies?
6. How does your country define "national security"? Is this concept used to restrict freedom of expression?
7. What is your country's ranking in the Freedom House and Reporters Without Borders rankings?
8. Does your country protect personal and biometric data through specific legislation?
9. Has your country signed the United Nations Convention against Cybercrime? Why?
10. Does your country export or import surveillance technologies? From which partners?
11. Are technology companies operating in your country required to share data with the authorities?
12. Does your country support binding international standards on digital rights, or does it prefer to maintain control at the national level?
13. For organizations and companies: What role can you play in protecting human rights online, and what are your limitations?

BIBLIOGRAPHY

Official documents :

UN, International Covenant on Civil and Political Rights, Art. 19, 1966. https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

UN, Resolution A/RES/73/179, The Right to Privacy in the Digital Age, 2018. https://digitallibrary.un.org/record/1661346

OHCHR, The Right to Privacy in the Digital Age. https://www.ohchr.org/fr/privacy-in-the-digital-age

UNESCO, Guidelines for the Governance of Digital Platforms, 2023. https://www.unesco.org/en/articles/guidelines-governance-digital-platforms

European Union, Regulation (EU) 2024/1689 (AI Act), EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

ECHR, Big Brother Watch, et al. v. United Kingdom, May 25, 2021. http://hudoc.echr.coe.int/eng?i=001-210077

PCLOB, *Report on the Telephone Records Program*, 2014. https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf

Reports and Studies

Freedom House, *Freedom on the Net 2025*. https://freedomhouse.org/sites/default/files/2025-11/Freedom_on_the_Net_2025_Digital.pdf

Buolamwini et Gebru, « Gender Shades », MIT Media Lab, 2018. https://proceedings.mlr.press/v81/buolamwini18a.html

NIST, *FRVT Part 3: Demographic Effects*, 2019. https://doi.org/10.6028/NIST.IR.8280

Carnegie Endowment, *The Global Expansion of AI Surveillance*, 2019. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance

Comparitech, *Surveillance camera statistics*.
https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

J. Penney, « Chilling Effects », *Berkeley Technology Law Journal*, 2016.
https://ssrn.com/abstract=2769645

Access Now, *Internet shutdowns in 2025*, 2026.
https://www.accessnow.org/internet-shutdowns-2025/

Top10VPN, *The Cost of Internet Shutdowns in 2025*.
https://www.top10vpn.com/research/cost-of-internet-shutdowns/

RSF, 2026 World Press Freedom Index. https://rsf.org/en/2026-rsf-index-press-freedom-25-year-low

Visual Capitalist, *Mapped: Press Freedom Around the World in 2026*.
https://www.visualcapitalist.com/mapped-press-freedom-around-the-world-in-2026/

Pew Research Center, *Key findings about Americans and data privacy*, 2023.
https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/

Press

ONU Info, *Sixty-five nations sign first UN treaty to fight cybercrime*, 2025.
https://news.un.org/en/story/2025/10/1166182