Committee: International Telecommunication Union
Issue: Defining international and future-oriented standards for the right to online privacy
Chairs: Charles Hermann Gomez, Antonio Badilla Olivas, Marit Pauwelyn

Defining international and future-oriented standards for the right to online privacy

ICTs for the SDGs:

The International Telecommunication Union is a UN organization whose mission is to standardize, harmonize and regulate the development of information and communication technologies (ICTs) in the world. One of its goals is to promote inclusiveness and universal access to these technologies. ITU is also collaborating with other UN organizations to effectively use ICTs to their full potential in order to achieve the Sustainable Development Goals (SDGs).

Introduction

We live in a world where everything is online. We could even say, we live online. All our conversations, research, ideas, experiences, opinions, friends, photos, songs we listen to on the bus, every piece of information that concerns us is absorbed by this incredibly complex space that is the Internet. As this space is now accessible almost worldwide, an individual's right to privacy is at stake at all times. This affects the ability to exercise almost all other rights, in particular freedom of expression and freedom of assembly and association. But online privacy does not only concern us individually, it's about how our government, but also other organizations and associations, use our information for their benefit. Indeed, governments have strengthened their ability to monitor citizen movements, censor speeches, block or filter access to information, and track communications to control our social, economic and social information and opinions. policies on the world. So how far will it go? How far will we live in a world where we soon have no right to be a mere individual? How can we, as an International Telecommunications Union, prevent this from going too far?

Key words

The right to privacy, how to define it universally?

It is crucial to start from the basis of the fundamental right to privacy which has been declared in Article 12 of the Universal Declaration of Human Rights:
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon their honor and reputation."

Of all human rights, privacy is perhaps the most difficult to define and illustrate. Definitions of privacy vary considerably through different contexts and environments. In many countries, the concept has been merged with data protection, which interprets privacy in terms of personal information management. Beyond this rather strict context, privacy is often seen as a means of determining how much society can interfere in someone's personal life. It is often divided into four categories:

- Confidentiality of information, which involves the establishment of rules governing the collection and processing of personal data, such as credit information and medical records;
- The protection of privacy, which concerns the protection of the physical person against invasive procedures such as drug testing and cavernous excavations;
- Confidentiality of communications, which covers the security and confidentiality of mail, telephones, emails and other forms of communication; and
- Territorial privacy, which concerns setting limits to intrusion into domestic and other environments, such as workplaces or public spaces.

Almost every country in the world explicitly recognizes the right to privacy in their constitutions. At a minimum, these provisions include the rights of inviolability of the home and confidentiality of communications. The most recent constitutions, such as those of South Africa and Hungary, include specific rights of access and control of personal information.

In many countries where privacy is not explicitly recognized in the Constitution, such as the United States, Ireland and India, judges have found this right guaranteed by other provisions. In many countries, international agreements recognizing the right to privacy, such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights, have been adopted.

More specifically, what is the right to privacy online?

Internet privacy, also known as online privacy, is a subset of data privacy and a basic human right. Indeed, it refers to the privacy to which an individual is entitled when displaying, storing or providing information about himself on the Internet. This can include both personal identification information (PII) and non-personally identifiable information (NPII), such as its behavior on a Web site. Without the confidentiality on the Internet, all its activities are likely to be gathered and analyzed by any interested parties!

What is personal data?

This concerns all information relating to an identified or identifiable physical person, directly or not, through an identifier or one or more elements specific to his identity.

It can be for example a name, a first name, an email address, a location, an ID card number, an IP address, a photo, a social or cultural profile.

Finally, what is an international standard?

During the debates, it will indeed be necessary to define international standards concerning the subject, ie resolutions that help each delegation and whose solutions are accessible and feasible for all. That's why they will be international.

General overview

The situation and current challenges

- ➔ **Where are the personal data stored?**

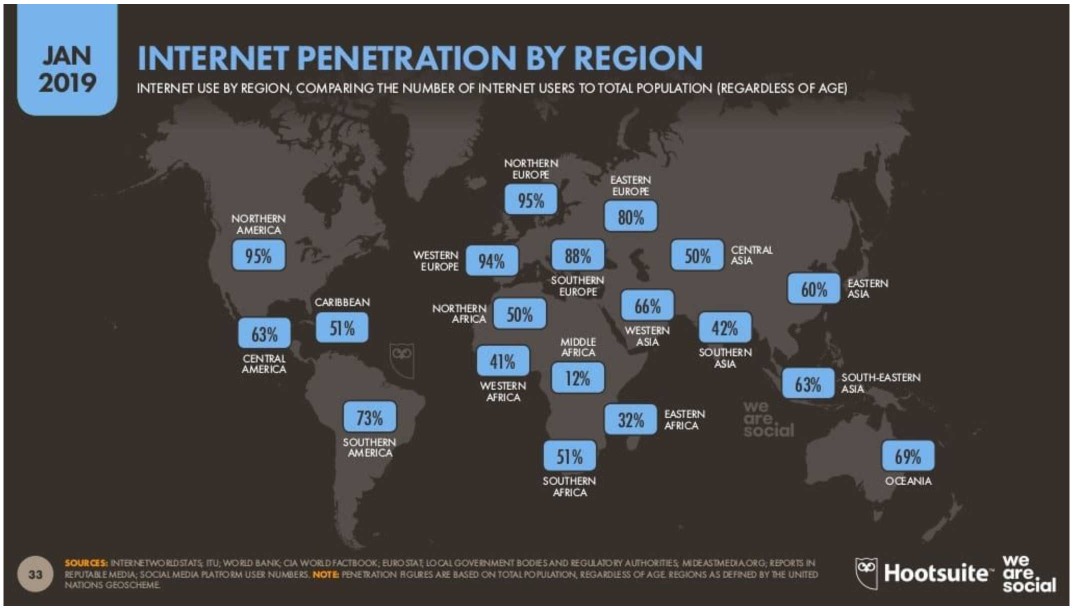
Online tools
Online tools have the ability to track and store location, information consumption, shopping patterns, social interactions, and even, via PDAs, the behavior and domestic discussions of their users. Here are some important tools that surround us daily:

1. **Social networks (PII)**

The naive use of social networks can lead to emotional, financial and legal consequences and, in some cases, to the disclosure or spreading of personal data. Kids and teens are already at risk on social networks, but adults, governments, banks, and even large Web businesses are not at all immune to risk either.

Social networks are more popular than ever. Of the world's 3.43 billion Internet users, 2.28 billion people (about one-third of the world's population) regularly visit social networks (a rising trend). Facebook, the platform that has the highest number of monthly clicks, is leading the pack and celebrates a double win among mobile users with its subsidiary WhatsApp.

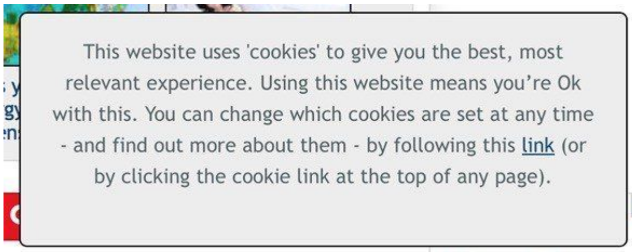
The user is not only a consumer, he is also an actor, he creates content (texts, videos, photos, ...) unlike the traditional Internet. Indeed, behind each social network, there are people who have access to all your data, even those so called "private". On the internet, you cannot control anything.
Social networks are full of hackers, cybercriminals and data vendors. When looking at this map, we can see that the internet is present throughout the world, in some countries more than in others. It also means that social networks play an important role worldwide, putting more than half of the global population at risk for invading privacy.


JAN 2019
INTERNET PENETRATION BY REGION
INTERNET USE BY REGION, COMPARING THE NUMBER OF INTERNET USERS TO TOTAL POPULATION (REGARDLESS OF AGE)
NORTHERN AMERICA 95%
CENTRAL AMERICA 63%
CARIBBEAN 51%
SOUTHERN AMERICA 73%
NORTHERN EUROPE 95%
WESTERN EUROPE 94%
SOUTHERN EUROPE 88%
EASTERN EUROPE 80%
NORTHERN AFRICA 50%
WESTERN AFRICA 41%
MIDDLE AFRICA 12%
EASTERN AFRICA 32%
SOUTHERN AFRICA 51%
WESTERN ASIA 66%
CENTRAL ASIA 50%
SOUTHERN ASIA 42%
EASTERN ASIA 60%
SOUTH-EASTERN ASIA 63%
OCEANIA 69%
33
SOURCES: INTERNETWORLDSTATS; ITU; WORLD BANK; CIA WORLD FACTBOOK; EUROSTAT; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; MIDEASTMEDIA.ORG; REPORTS IN REPUTABLE MEDIA; SOCIAL MEDIA PLATFORM USER NUMBERS. NOTE: PENETRATION FIGURES ARE BASED ON TOTAL POPULATION, REGARDLESS OF AGE. REGIONS AS DEFINED BY THE UNITED NATIONS GEOSCHEME.
Hootsuite
we are social

(https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/)

1. The use of cookies (NPII)

Cookies, also known as online witnesses, have been on the internet for more than 20 years. They make it possible to retain user data during a connection, in order to facilitate navigation to the Internet users. They have different functions in particular in the case of an e-commerce activity to store the contents of a shopping cart, to record the language settings of a website, or in a more commercial purpose, to create targeted advertising. However, cookies have always been more or less controversial because these text files contain personal information that can potentially be exploited by third parties, which can lead to a risk in terms of security.

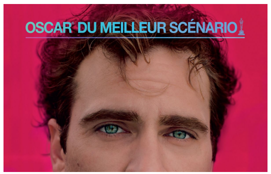


This website uses 'cookies' to give you the best, most relevant experience. Using this website means you're Ok with this. You can change which cookies are set at any time - and find out more about them - by following this link (or by clicking the cookie link at the top of any page).

There is a regulation to secure the privacy of the user, which insists on the consent of the individual before the deposit of cookies, the communication on the purpose of these cookies and a way to decline the use of them. However, this consent is only valid for a maximum of 13 months.

(Https://www.termsfeed.com/blog/4-ways-notify-users-cookies/)

However, there are many dangers and risks in accepting these cookies. Indeed, they facilitate the work of hackers, whose goal is for them to exploit the content and use this personal data for malicious purposes that can go as far as the establishment of cyber attacks. For example, the NSA (National Security Agency) uses these cookies to monitor the lives of Internet users, as revealed by the documents published in December 2013 by Edward Snowden. According to the Washington Post, the technique used by the NSA and the BIA, the British intelligence agency, is to obtain PREF cookies, specific to Google, to identify targets and monitor their navigation. In the name of national protection and under the guise of the "Patriot Act", this set of laws that



compel US companies to provide the desired information, the NSA has granted the right of access to this information.

2. Digital personal assistants (NPII)

Mostly present in smartphones, these tools, better known under the names of Siri, Alexa, Google Assistants or Cortana, are often hidden in a speaker and serve as a domestic assistant. Thanks to their artificial intelligence, they answer questions or orders from their owner after hearing the specific call expected by the machine.
(image: HER film, dealing with a love affair between a man and a personal assistant: http: //www.allocine.fr/film/fichefilm-206799/dvd-blu-ray/? cproduct = 374684)

More and more doubts arise about the intention of these "assistants", many theories have been formed saying that they are extremely dangerous and may do more than just react to the needs of humans. Normally, these devices are triggered when the user pronounces the expected keyword ("Alexa", "OK Google" etc.). Before this keyword, they "listen", but in principle do not send any information on the network. After the keyword, conversations are sent to the cloud to process the order. Amazon, Google or Apple ensure that the data is encrypted and there is no random listening. Whatever the companies say, "*behind the voice assistants, people can hear you*," warns *The Quadrature of the Net*, who defend freedom in the digital world. Indeed, human beings help machines to become intelligent by listening to and verifying the transcripts of spoken words. Are personal assistants not just domestic helpers but government spies? There have been many incidents that seem to justify these ideas, but the creators still seem to find an explanation. Does this invention surpass the limits of the private life of an individual? Who should have to decide these regulations?

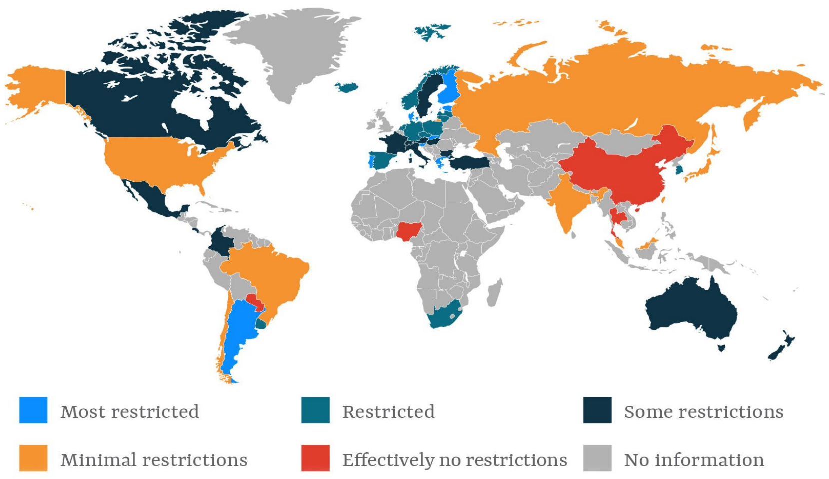
➔ What laws are in place to limit the use of this personal data?

As stated earlier in the report, almost all countries recognize the right to privacy and protect it through their laws. But what legislative framework has been established at an international level?

Worldwide, a general movement for the adoption of laws that relies for the most part on the models put in place by the Organization for Economic Cooperation and Development (https://www.oecd.org/ en /) and the Council of Europe (https://www.coe.int/en/) is underway.

In 1995, aware of both the deficiencies of the law and the many differences in the level of protection in each of its states, the European Union adopted a European directive that offers citizens a more varied and detailed protection against misuse of their rights to data.

The Directive requires the Member States to ensure that personal data relating to European citizens are covered by the law when exported to, or processed in, countries outside Europe. This requirement has led to increasing pressure on other governments, leading to more than forty other countries introducing data protection or information privacy laws. Others are in the process of adoption.



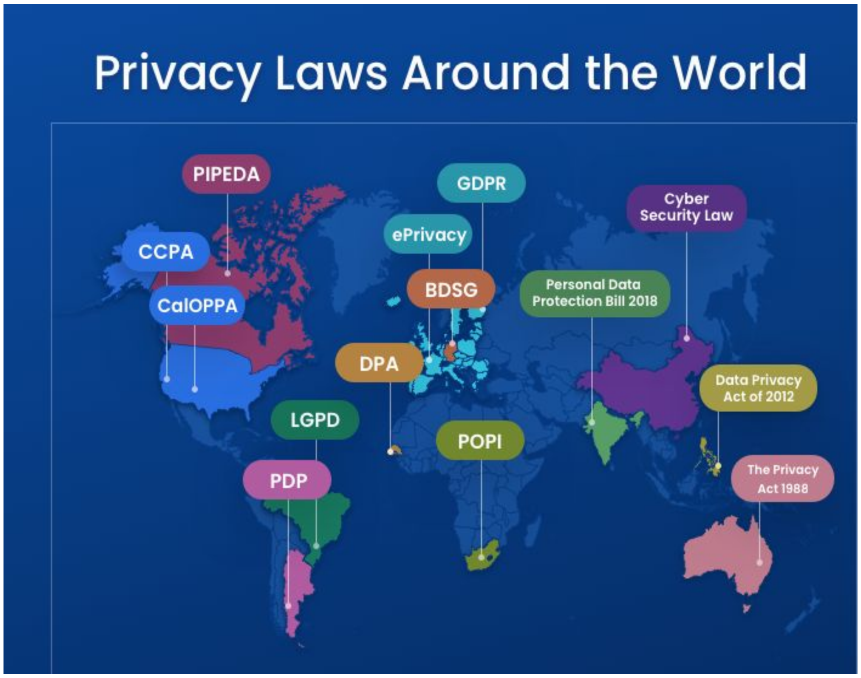
Privacy and data protection by country

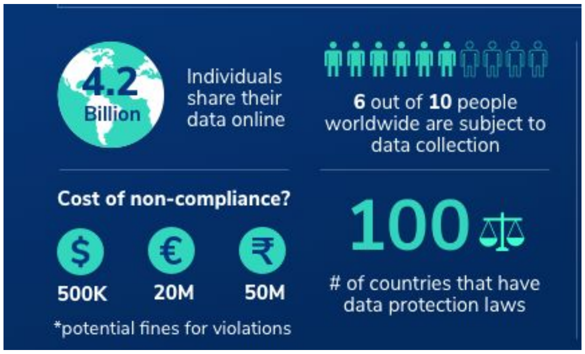
Source: Forrester

Why adopt exhaustive laws?

- To remedy past injustices. Many countries, including Central Europe, South America and South Africa, are passing laws to address privacy abuses committed under previous authoritarian regimes.
- To promote e-commerce. Countries, such as those in Asia, but also in Canada, have developed or are developing legislation to promote e-commerce. These countries recognize that consumers are uncomfortable with sending their personal information around the world. Privacy laws are part of a set of laws designed to facilitate electronic commerce by establishing uniform rules.
- To ensure that laws are compatible with pan-European laws. Most Central and Eastern European countries are adopting new laws based on the Council of Europe Convention and the EU Directive on data protection. Some hope to join the European Union in the near future, others, like Canada, are adopting new laws to ensure that trade will not be affected by the requirements of the EU directive.

(Http://gilc.org/privacy/survey/intro.html)





4.2 Billion Individuals share their data online

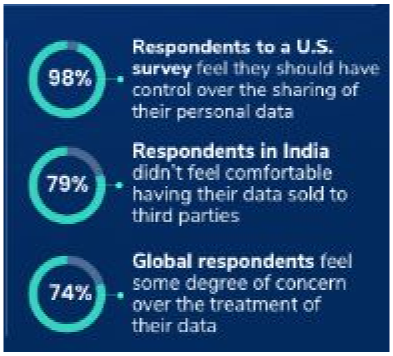
6 out of 10 people worldwide are subject to data collection

Cost of non-compliance?

$ 500K € 20M ₹ 50M

*potential fines for violations

100 # of countries that have data protection laws



98% **Respondents to a U.S. survey** feel they should have control over the sharing of their personal data

79% **Respondents in India** didn't feel comfortable having their data sold to third parties

74% **Global respondents** feel some degree of concern over the treatment of their data

➔ What are the stakes of these laws?

- The **intense development of technology**, which introduces more and more machines that can collect, analyze and disseminate data at an incredible speed, creates many confusions and gaps in protection laws, and also creates proportionately more potential for invasion of privacy. With this growth, the urgent situation is only getting worse.
- New developments in research and medical care, telecommunications, advanced transportation systems and financial transfers have significantly increased the level of information generated by each individual.
- **Globalization** removes geographic limitations to the data flow. The development of the Internet is perhaps the best-known example of a globalized technology.
- Convergence, due to the development of technology, leads to the elimination of technological barriers between systems. Modern information systems are increasingly linked with other systems and can exchange and process different forms of data.
- In some countries, agencies and associations have had a lot of exemptions regarding the application of confidentiality laws
- Without supervision and enforcement, **laws are sometimes simply ignored**.

More than 90 countries are **illegally controlling the conversations** of political opponents, human rights defenders, journalists and union organizers.

Police services, even in countries with strong privacy laws like Norway or Sweden, still **keep many cases** of citizens not charged or even suspected of crime

In Japan, police recently fined 2.5 million yen for **illegally listening to members of the communist party**

In France, a government commission estimated in 1996 that there were more than 100,000 **telephone recordings** made by private actors, often on behalf of public bodies.

In the United States, despite the existence of a consumer credit information law, businesses continue to **use this information for marketing purposes.**

The impact of the invasion of privacy on the population

It has always been difficult to define what impact results from a violation of an individual's privacy. What is the real difference between someone entering your home without permission and the state that listens to a personal phone conversation? It is increasingly difficult to answer this question now that data collection and processing initiatives have developed and are no longer focused only on specific individuals, but on society as a whole. What does one do wrong by collecting data on an entire population or by recording with surveillance cameras the daily lives of citizens at the corner of almost every street? How can these damages be taken into account without material evidence or specific quantities?

Once an individual is online, he becomes enormously vulnerable by exposing himself to many risks and uncertainties: who could use his information, for what, and for how long? Respecting privacy means respecting the standards of what information is taken into account, how it is used and with whom it is shared.

In this technological era, the concept of harm becomes more and more problematic. Often, an individual is simply unaware that his / her personal data is used by citizens (social networks), businesses (the use of cookies), or by the government (surveillance, eg cameras). If an individual goes to court to defend his rights, how could he accuse anyone? What specific harm has the National Security Agency (NSA) done to an American or any citizen?

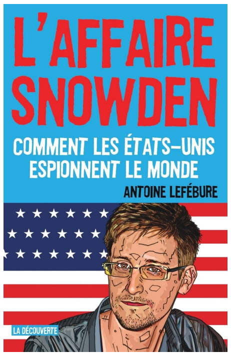
The courts have fought hard against this controversial issue, and little progress has been made. We desperately need a better understanding and approach to these violations.

Here are some examples of its impacts on the population:

- The exposure of their data caused them emotional distress.
- The exposure of their data has exposed them to an increased risk of harm related to identity theft, fraud or other injuries.
- The exposure of their data forced them to spend time and money to avoid future fraud, such as registering for credit monitoring, contacting credit reporting agencies, placing fraud on their accounts, etc.
- The collection or use of data without consent or without their knowledge

Courts often do not accept these arguments because there is no valid evidence, or the explanation seems to be too personal and abstract. These impacts are therefore in most countries completely ignored.

Case studies



The Snowden Case

From Wikileaks to the “Paradise Papers”, the last decade has been marked by a proliferation of revelations from large leaks of confidential documents. The Snowden affair, which broke out in 2013, concerned Edward Snowden, a security analyst for a subcontractor of the NSA, but especially the biggest hacker of his time, who leaked tens of thousands of NSA documents describing the massive surveillance program from the US agency.

Here are some revelations:

- Several mass surveillance programs, telephone calls and online exchanges set up by the NSA.
- The US agency has allowed itself to eavesdrop on many foreign leaders. (for example the last 3 French Presidents)
- Many data are collected on ordinary citizens in the United States.
- The NSA is obviously monitoring for the purpose of counter-terrorism, but also in economic and industrial espionage.

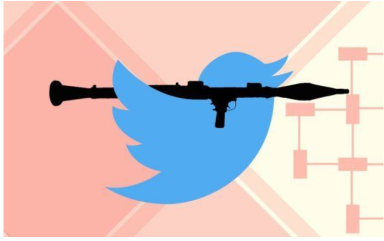
After these revelations, there was a shock not only for the Americans, but for the entire world. This event was in a way a symbol of the beginning of this technological era where all the data is supervised and recorded.

(Http://www.leparisien.fr/international/tout-comprendre-a-l-affaire-snowden-07-11-2017-7378926.php)

The famous "cyber-jihadist" branch

The use of the Internet for terrorist purposes is a growing phenomenon.

The Internet can be used not only to publish persuasive and extremist videos, but also to build relationships with, and solicit support from, those most receptive to propaganda.



Terrorist organizations are increasingly using propaganda on platforms such as password-protected websites or restricted-access newsgroups to recruit illegally. The reach of the Internet offers terrorist organizations and their supporters a worldwide pool of potential recruits.

Access- restricted cyberforums provide recruits with a place to learn about, support and participate directly in terrorist-related actions. The use of technological locks at the entrance to recruitment platforms also makes it difficult for intelligence and law enforcement personnel to monitor terrorist activity.

As an example : Twitter

Twitter "was a platform of choice for jihadists"

This positioning took a massive turn in the late 2000s with the advent of social networks Facebook, Youtube, Twitter. So far, jihadists have mostly occupied websites and forums. In 2014, the Islamic State group is at its peak on the networks. Thousands of accounts broadcast jihadist content en masse on many platforms. The awareness took a turn with the attack of Charlie Hebdo in January 2015.
https://www.google.fr/amp/s/www.franceculture.fr/amp/numerique/twitter-etait-une-plateforme-de-choix-pour-les-djihadistes

Possible solutions

- **Clarify and affirm the instauration of international laws already in place**: systematically review government policies on digital communications and the collection of personal data, and find policies that violate privacy without valid justification;
- **Ensure that all national laws on online privacy respect human rights:** verify that national privacy laws and procedures are compatible with the obligations of the Universal Declaration of Human Rights ;
- **Examine the responsibilities of the private sector**: by following the "Protect, Respect and Repair" framework of the UN Guiding Principles, in the specific context of digital information and communication technologies;
- **Encourage international standards that treat privacy as a right:** see the link between privacy, freedom of expression and other human rights in the digital context;
- **Working with UN experts:** on the protection of freedom of expression, freedom of assembly and association and human rights defenders, on the identification of specific rights-related threats in the context of mass surveillance, on a more comprehensive approach to privacy protection
- **Stimulate the platforms (eg Facebook, Twitter, Instagram) to engage more concretely:** in the follow-up of the reports of their users, in the possible development of AI preventing the hackers and piracy before action, and in their cooperation with the cybercrime policies. More concretely, as soon as a feedback is done by a user, it must be analyzed / is answered as soon as possible. And commitments, between the country with its laws and the platform can be established (example: an AI detecting scenes of violence, for an immediate suppression)

Important countries and organisations

Algeria : this country does not have private data laws, so can use them freely because it is not restricted by any framework.

Spain: country where personal data are framed by the GRDP (General Regulation on Data Protection) so protected, and does not have tools for transfers.

The NCIL (National Commission on Information and Liberty)

This very detailed map allows you to view the different levels of data protection in countries around the world:https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

DIGIT (European Commission Directorate General for Informatics)

This page details the responsibilities of the commission at a European level:
https://ec.europa.eu/info/departments/informatics/mission-statement-informatics_fr

Questions to ask yourselves

- How can we define universal limits to the invasion of privacy on the internet?
- What standards can be put in place that will be applicable for any government (with both countries that depend heavily on online control and others not at all)
- How can we strengthen existing laws so that they are not ignored?
- Knowing that solutions must be "future-oriented", how can we take into account the constant and rapid development of technology in our debates and resolutions? What should we then emphasize or clarify so that there are no misunderstandings or forgotten elements?
- How can we explain the risks of social media that are both personal but also ethical and political? How can we reduce them?

Bibliography

https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy
https://www.un.org/fr/universal-declaration-human-rights/
http://gilc.org/privacy/survey/intro.html
https://www.francetvinfo.fr/internet/amazon/faut-il-se-mefier-des-assistants-vocaux-trois-exemples-d-espionnage-qui-incitent-a-la-prudence_2771149.html
https://www.jipitec.eu/issues/jipitec-8-4-2017/4641/
https://teachprivacy.com/privacy-data-security-violations-whats-harm/
Service public pro
https://www.service-public.fr/professionnels-entreprises/vosdroits/F24270

Le petit juriste
https://www.lepetitjuriste.fr/la-protection-des-donnees-personnelles-sur-internet/

https://www.contrepoints.org/2019/07/22/349557-internet-il-faut-proteger-votre-vie-privee https://www.google.fr/amp/s/sawisms.blog/2016/10/09/dangers-reseaux-sociaux-vie-privee/amp/

https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

https://www.fnac.com/5-conseils-pour-proteger-sa-vie-privee-sur-le-net/cp38684/w-4

Europea.Eu
https://www.google.fr/amp/s/europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/indexamp_fr.htm

Can we really protect ourselves?
https://www.legavox.fr/blog/alexandre-chombeau/atteinte-privee-internet-peut-vraiment-21846.htm

The use of Internet UNODC :
https://www.unodc.org/documents/congress/background-information/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf