



# **Human Rights in the Digital Age**

## **V lecture: Protection of specific rights in the digital age**

**Visiting prof. dr. Dovile Gailiute-Janusone**



# Outline

1. Cyber torture
2. Digital discrimination, Cyber racism
3. Cybercrimes and human rights
4. Cybersecurity and human rights
5. Children rights in the digital environment
6. Effective remedies for restriction or violation of rights online







**Prohibition of torture**



# International instruments

● 1948 Universal Declaration of Human Rights, Art. 5

● The four 1949 Geneva Conventions

● 1966 UN International Covenant on Civil and Political Rights, Art. 7

● 1984 UN Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment

● 1987 European Convention for the Prevention of Torture and Inhuman and Degrading Treatment or Punishment

● 1998 Rome Statute of the International Criminal Court

Prohibition of torture is also part of customary international law, and is considered to be *jus cogens*



## **Article 3 of the ECHR:**

*No one shall be subjected to torture or to inhuman or degrading treatment or punishment.*



Could police officers threaten to torture a suspect if they believe this may save the life of an innocent people?

## The absolute character of Art. 3

The Court has emphasised that Article 3 is absolute regardless of either:

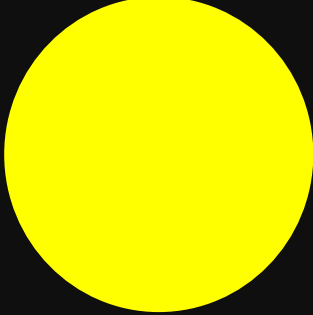

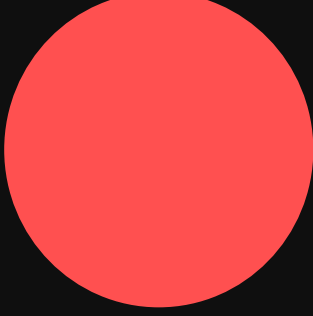
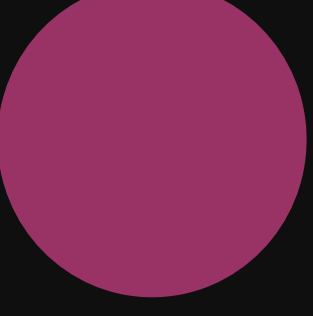
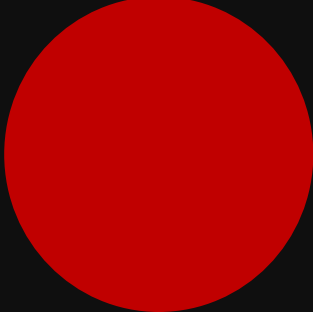
- the conduct or circumstances of the victim or the nature of any offence or
- the nature of any threat to the security of the State.

# Scope of Art. 3

X

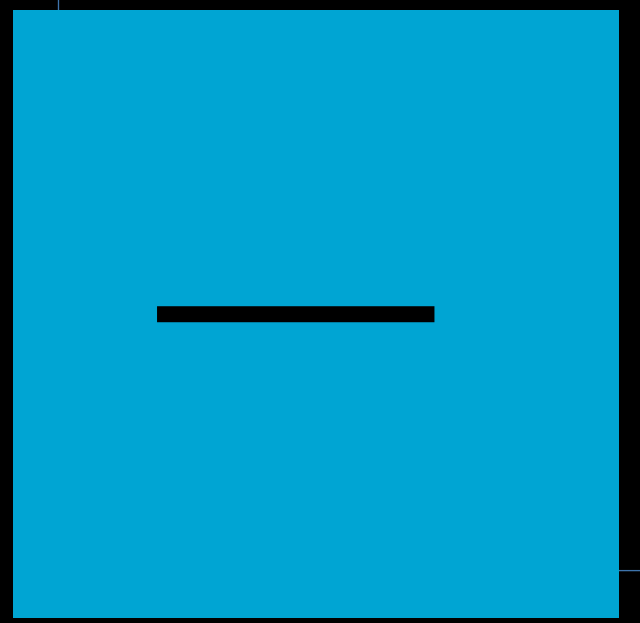
 not all ill-treatment or punishment is prohibited, the treatment in order to fall within the scope of Article 3 it must attain a minimum level of severity.

 The assessment of this minimum depends on all the circumstances of the case, such as:

-  nature and context of the treatment or punishment
-  manner and method of its execution
-  its duration
-  its physical or mental effects
-  in some instances, the sex, age and state of health of the victim

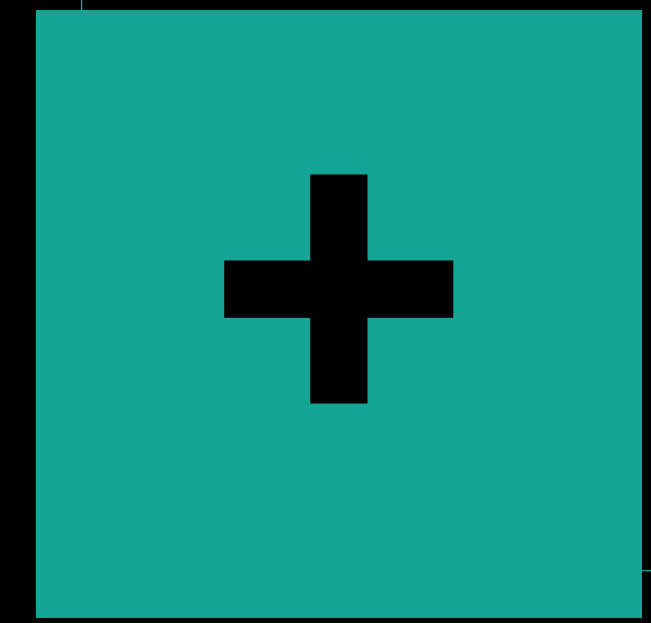


# Article 3 comprises both positive and negative aspects

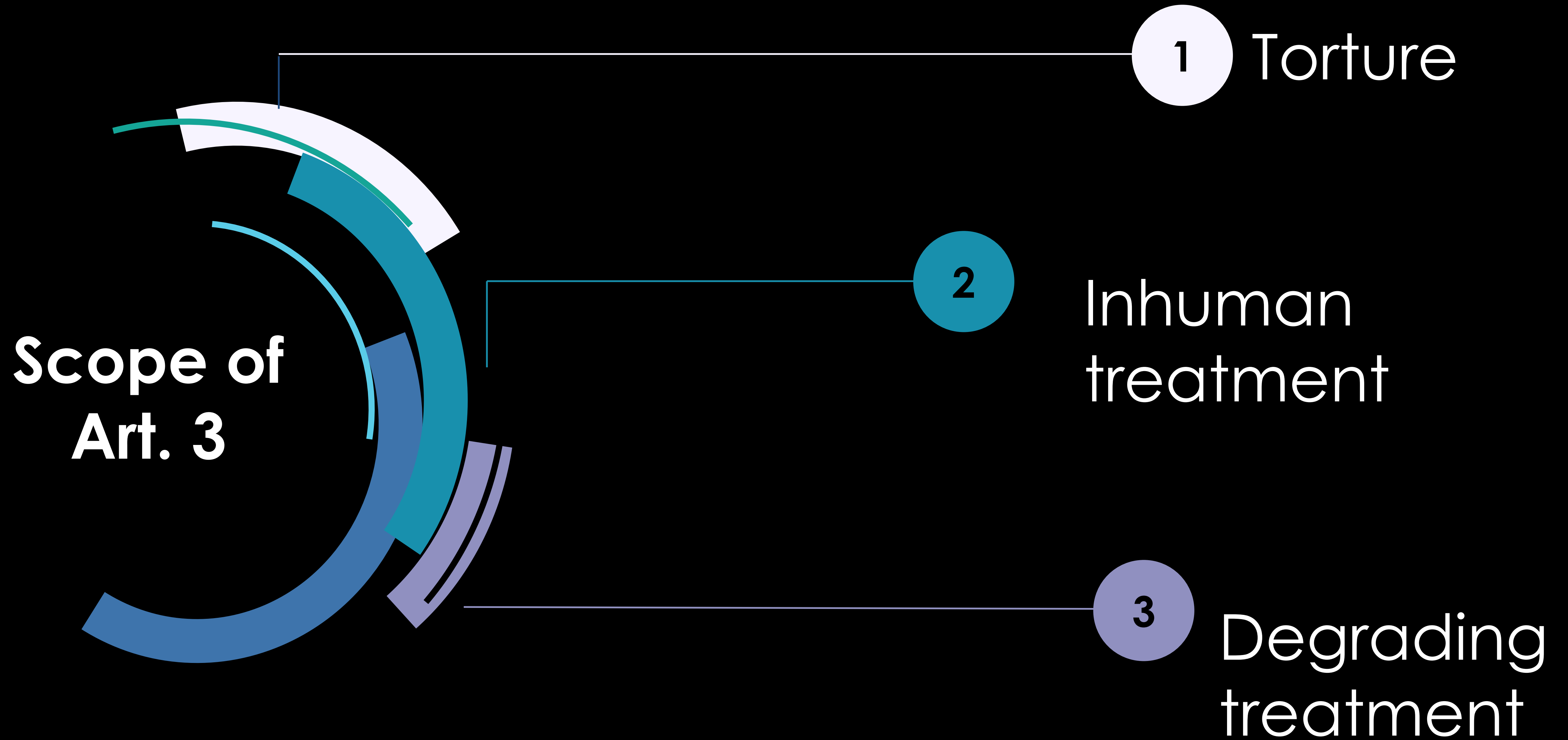


to refrain from acts of torture and other forms of ill-treatment foreseen in Article 3. (also 'principle of non-refoulement')

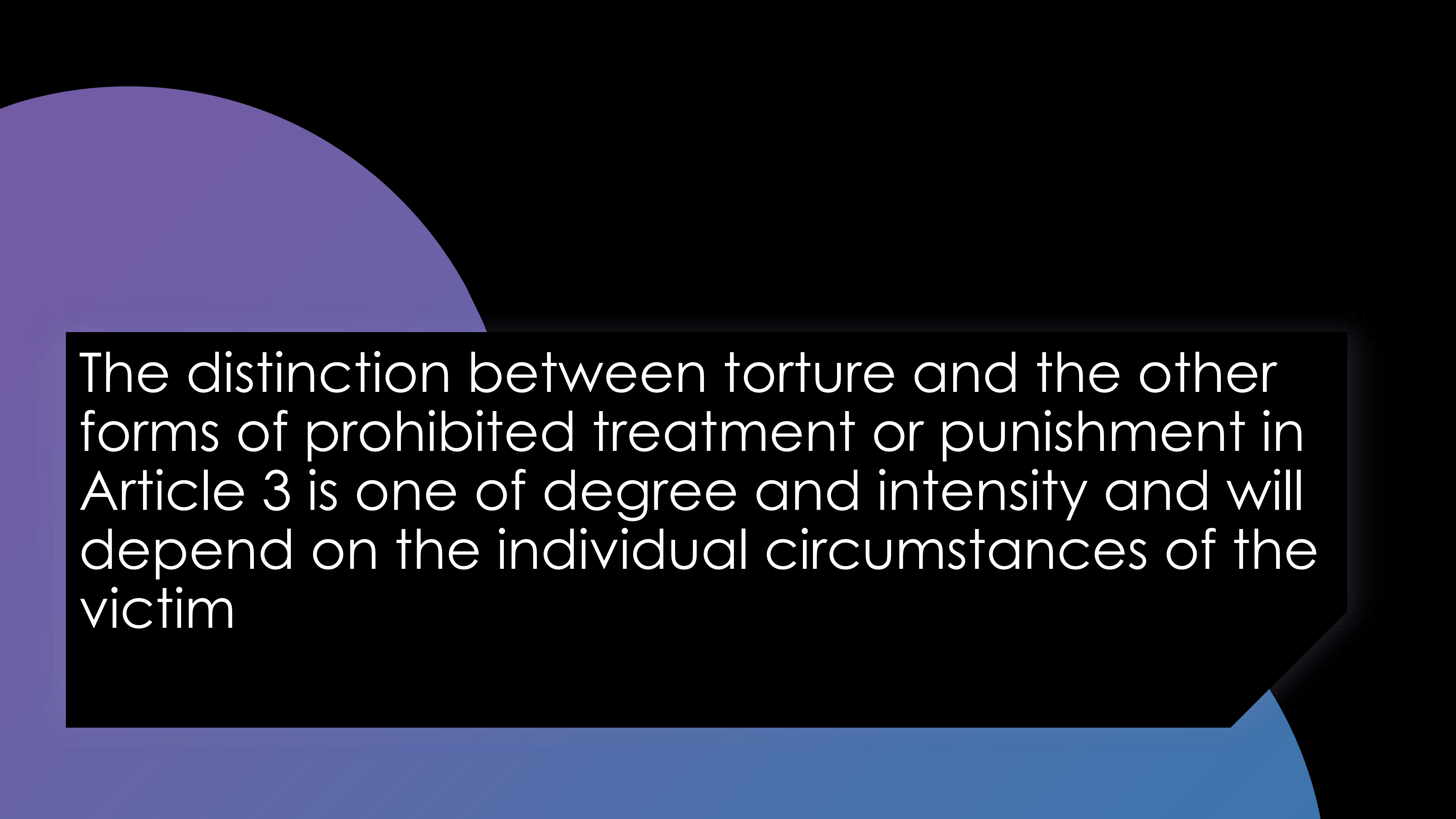
Article 3, requires States to take measures designed to ensure that individuals within their jurisdiction are not subjected to ill-treatment administered not only by State agents but also by private individuals (see *Z and Others v. the United Kingdom* [GC], no. [29392/95](#)).



to secure the right to be free from torture and other forms of ill-treatment







The distinction between torture and the other forms of prohibited treatment or punishment in Article 3 is one of degree and intensity and will depend on the individual circumstances of the victim

# Definition of torture

- A useful definition of torture can be found in the **UN Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984)**. **Article 1 states:**
- For the purposes of this Convention, the term “torture” means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions.

**Definition is not binding to the European Court of Human Rights**



# Essential elements which constitute torture

**Intensity**


infliction of  
severe mental  
or physical pain  
or suffering

**Intension**

the intentional  
or deliberate  
infliction of the  
pain

**Purposive  
treatment**

pursuit of a  
specific purpose,  
such as gaining  
information,  
punishment or  
intimidation



Subject – “*is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity*” (G.R.B. v. Sweden; Opuz v. Turkey)




Fault requirement – “*intentionally inflicted*” (Ireland v. UK, Nevmerzhitsky v. Ukraine)



Special purpose requirement (*Prosecutor v. Zejnil Delalic, Zdavko Mucic; Prosecutor v. Milorad Krnojelac*)



Act/Omission – “*any act*”



Consequences – “*severe pain or suffering, whether physical or mental*” (Ireland v. UK; Aksoy v. Turkey; Aydin v. Turkey)



Owing to the absolute character of the right guaranteed, the Court does not rule out the possibility that Article 3 of the Convention may also apply where the danger emanates from persons or groups of persons who are not public officials. However, it must be shown that:

- the risk is real and
- the authorities of the receiving State are not able to obviate the risk by providing appropriate protection.

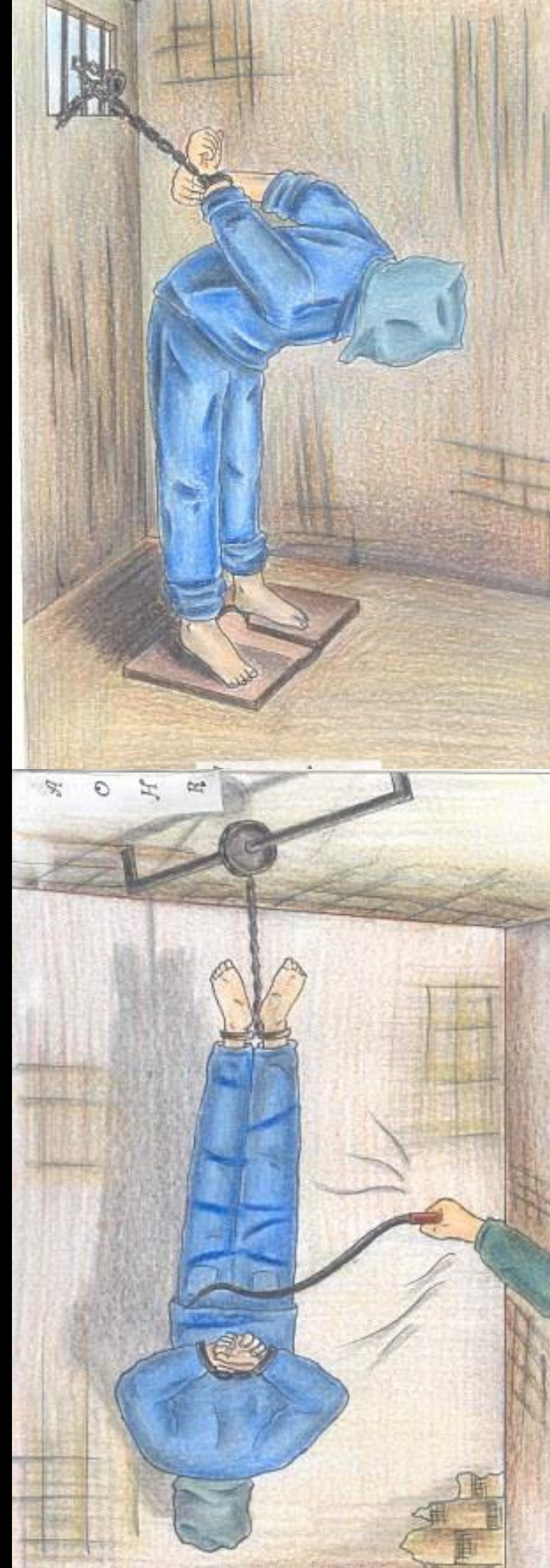
Documents from various sources produced in support of the applicant's memorial provide insight into the tense atmosphere in Colombia, but do not contain any indication of the existence of a situation comparable to his own. Although drug traffickers sometimes take revenge on informers, there is no relevant evidence to show in H.L.R.'s case that the alleged risk is real. His aunt's letters cannot by themselves suffice to show that the threat is real. Moreover, there are no documents to support the claim that the applicant's personal situation would be worse than that of other Colombians, were he to be deported.

**H.L.R. v. France, no. 24573/94, 29/04/1997**



## Examples of torture:

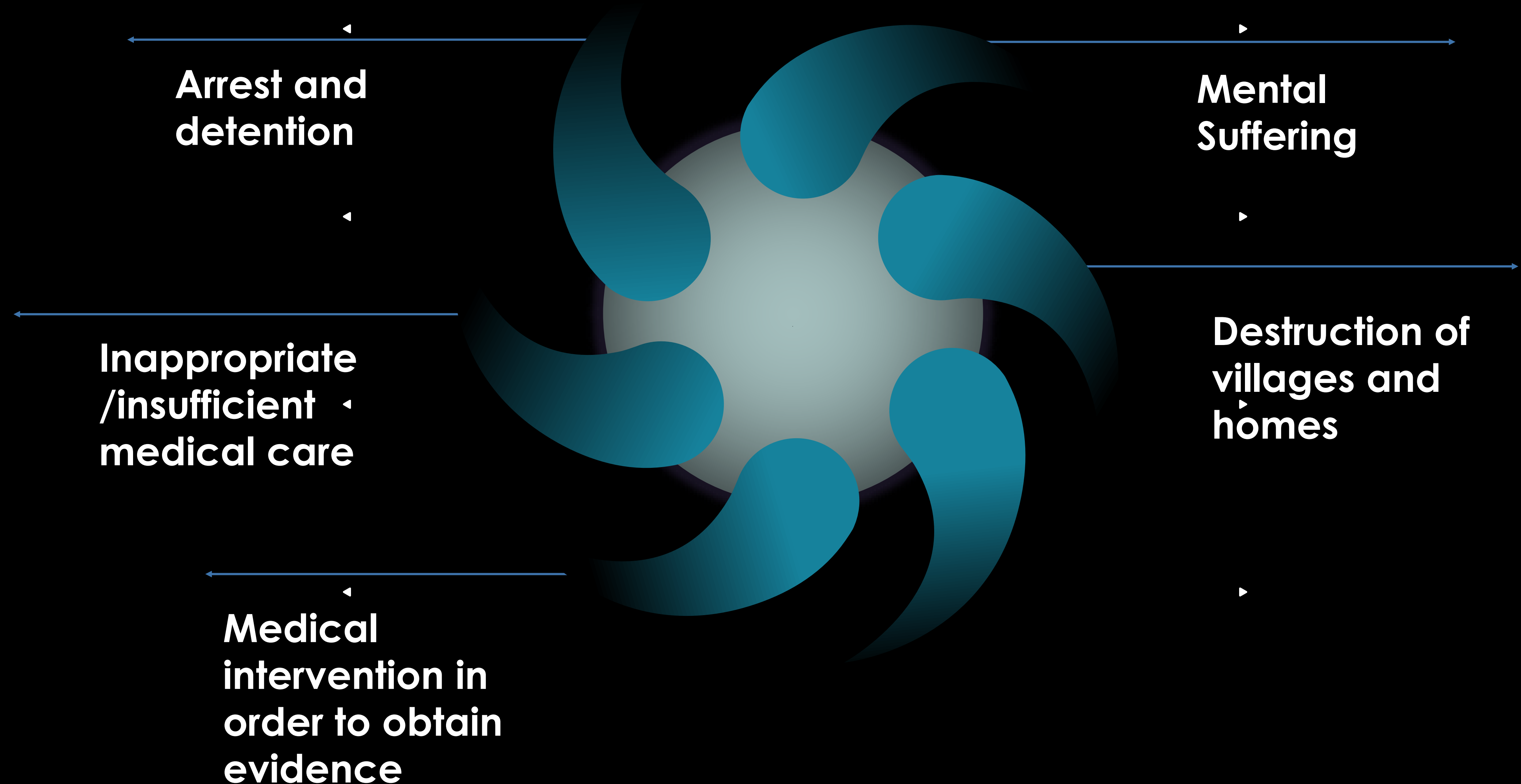
- “Palestinian hanging”
- Electric shocks
- Combination of torture methods
- Beating, threats against life and family, sexual intimidation and humiliation
- Accumulation of circumstances: fear of execution, detention conditions, no medical treatment
- Forced feeding in a particularly violent and humiliating manner
- Rape (and/or threat of rape)





- The distinction between torture and inhuman treatment derives principally from a difference in the intensity of the suffering inflicted. (*Ireland v United Kingdom*, para. 167).
- In addition, while torture on the one hand generally requires the proof of a particular purpose as outlined above, the other forms of ill-treatment do not.
- The Court has considered treatment to be “inhuman” when, *inter alia*, it was *premeditated*, was applied for hours at a stretch and caused either actual bodily injury or intense physical and mental suffering.
- The Court has deemed treatment to be “degrading” when it was such as to arouse in the victims feelings of fear, anguish and inferiority capable of humiliating and debasing them.

# Examples of inhuman treatment







- ❖ Where a person is injured while in detention or otherwise under the control of the police, any such injury will give rise to a strong presumption that the person was subjected to ill-treatment (see *Bursuc v. Romania*, no. 42066/98, § 80, 12 October 2004, *Gurgurov v. Moldova*, no. 7045/08, § 55, 16 September 2009).
- ❖ It is incumbent on the State to provide a plausible explanation of how the injuries were caused, failing which a clear issue arises under Article 3 of the Convention
- ❖ In assessing evidence, the Court has generally applied the standard of proof “beyond reasonable doubt” (see *Ireland v. the United Kingdom*, 18 January 1978, § 161, Series A no. 25).
- ❖ Where the events in issue lie wholly, or in large part, within the exclusive knowledge of the authorities, as in the case of persons within their control in custody, strong presumptions of fact will arise in respect of injuries occurring during such detention. Indeed, the burden of proof may be regarded as resting on the authorities to provide a satisfactory and convincing explanation (see *Salman v. Turkey* [GC], no. 21986/93, § 100, ECHR 2000-VII).

**Proving ill-treatment**



# Conditions of detention

The State has to ensure that all prisoners were detained in conditions which respected their human dignity, that they are not subjected to distress or hardship of an intensity exceeding the unavoidable level of suffering inherent in detention and that their health is not compromised.

In cases concerning prisoners' living space, the Court established a minimum threshold of 3 sq. m of personal space. Where the space provided is above that threshold the Court takes other factors, such as standards of hygiene, into consideration.



# Conditions of detention

State has a duty of care towards sick prisoners, comprising three specific obligations:

- State has to be satisfied that the person concerned was fit to be detained;
- State is required to provide prisoners with the medical care they needed;
- State has to adapt the overall conditions of detention of the person concerned as necessary to his or her particular state of health.







## Migrants' Detention

In certain cases, conditions of extreme poverty of vulnerable individuals, such as asylum seekers, may amount to a violation of Article 3 ECHR

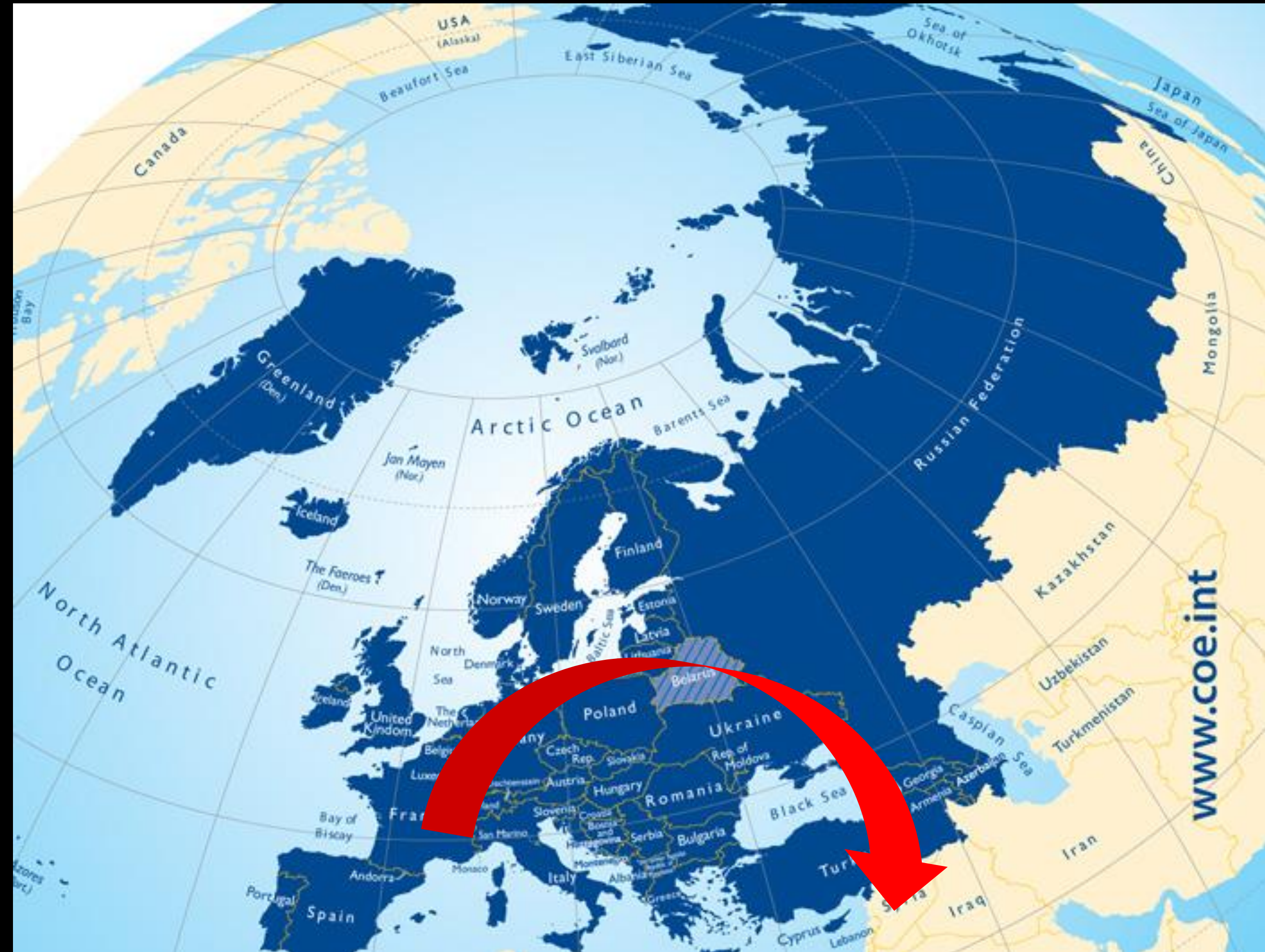
**M.S.S. v. Belgium and Greece:** the applicant had been living in the street for several months "with no resources or access to sanitary facilities, and without any means of providing for his essential needs", that he had been a "victim of humiliating treatment showing a lack of respect for his dignity", that he was undoubtedly subject to "fear, anguish or inferiority capable of inducing desperation"





# Expulsion

Expulsion by a Contracting State may give rise to an issue under art. 3, and hence engage the responsibility of that State, where substantial grounds have been shown for believing that the person in question, if expelled, would face a real risk of being subjected to treatment contrary to art. 3 in the receiving country.



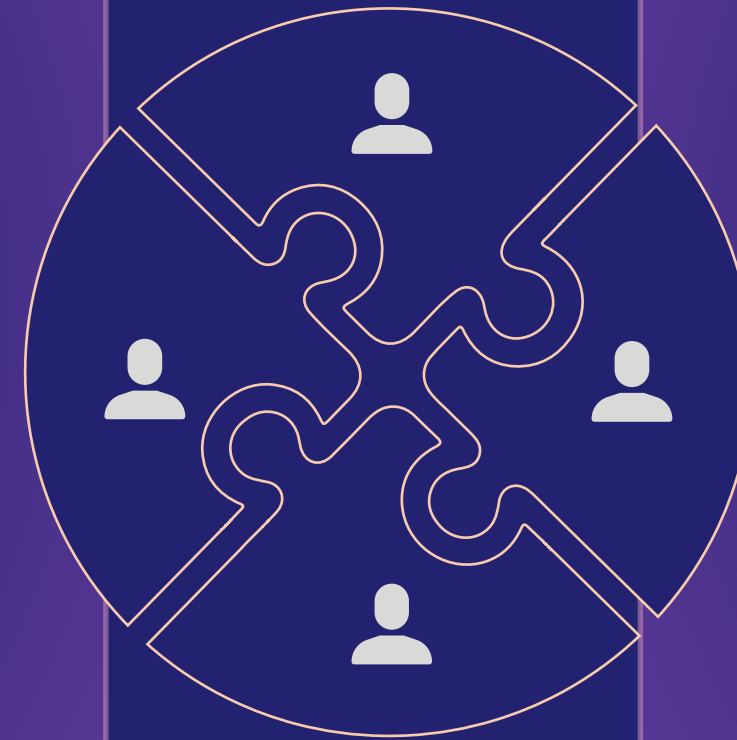


## Cybertorture: terminology

Inconsistent terminology is one of the major challenges to assessing how cyber-technologies can be used to commit harmful or violent acts. It is unsurprisingly difficult to try and comprehend any definite legal distinctions between terms like cyber-abuse, cyber-harassment, cyber-harm, cyber-ill-treatment, cyber-bullying, cyber-violence, cyber-crime, and cyber-torture.

# Types of cyberviolence

Violence that is  
committed through  
cyber-technologies



Violence that is  
enabled by cyber-  
technologies



There are no legal standards nor any case law directly addressing acts of torture or ill-treatment through cyber-technologies.

**Cybertorture** - possible use of various forms of information and communication technology (“cybertechnology”) for the purposes of torture.



# Cybertorture

States, corporate actors and organized criminals not only have the capacity to conduct cyberoperations inflicting severe suffering on countless individuals, but may well decide to do so for any of the purposes of torture.

In practice, cybertechnology already plays the role of an “enabler” in the perpetration of both physical and psychological forms of torture, most notably through the collection and transmission of surveillance information and instructions to interrogators, through the dissemination of audio or video recordings of torture or murder for the purposes of intimidation, or even live streaming of child sexual abuse “on demand” of voyeuristic clients, and increasingly also through the remote control or manipulation of stun belts, medical implants and, conceivably, nanotechnological or neurotechnological devices

Cybertechnology can also be used to inflict, or contribute to, severe mental suffering while avoiding the conduit of the physical body, most notably through intimidation, harassment, surveillance, public shaming and defamation, as well as appropriation, deletion or manipulation of information

# Cybertorture

Electronic communication services, social media platforms and search engines provide an ideal environment both for the anonymous delivery of targeted threats, sexual harassment and extortion and for the mass dissemination of intimidating, defamatory, degrading, deceptive or discriminatory narratives.

Individuals or groups systematically targeted by cybersurveillance and cyberharassment are generally left without any effective means of defence, escape or self-protection and, at least in this respect, often find themselves in a situation of “powerlessness” comparable to physical custody.


Depending on the circumstances, the physical absence and anonymity of the perpetrator may even exacerbate the victim's emotions of helplessness, loss of control and vulnerability, not unlike the stress-augmenting effect of blindfolding or hooding during physical torture.

# Cybertorture


Generalized shame inflicted by public exposure, defamation and degradation can be just as traumatic as direct humiliation by perpetrators in a closed environment

Much more systematic, government-sponsored threats and harassment delivered through cyber-technologies not only entail a situation of effective powerlessness but may well inflict levels of anxiety, stress, shame and guilt amounting to “severe mental suffering”, as required for a finding of torture



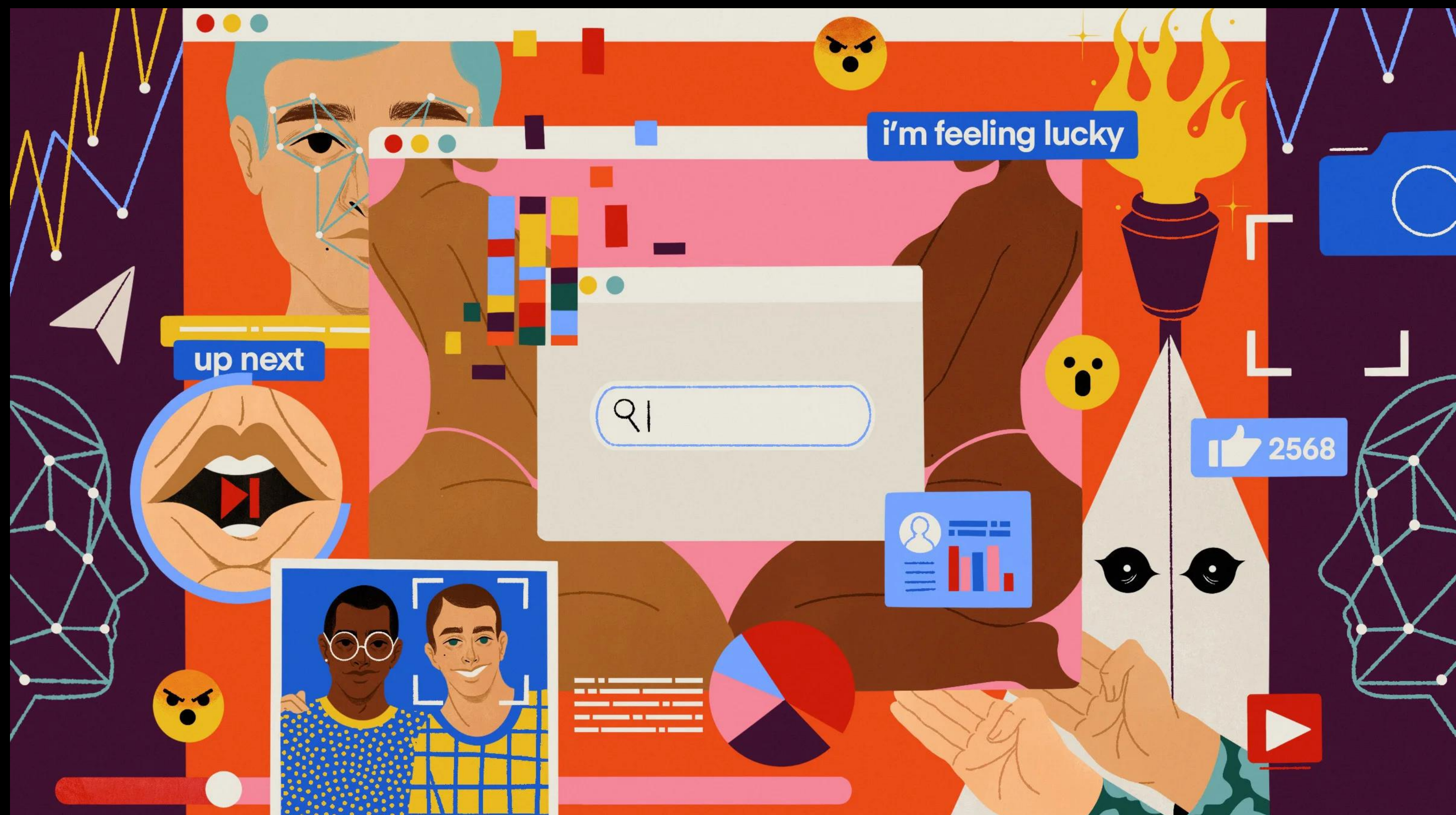


In order to ensure the adequate implementation of the prohibition of torture and related legal obligations in present and future circumstances, its interpretation should evolve in line with new challenges and capabilities arising in relation to emerging technologies not only in cyberspace, but also in areas such as artificial intelligence, robotics, nanotechnology and neurotechnology, or pharmaceutical and biomedical sciences, including so-called “human enhancement”.





# Digital discrimination



# Prohibition of discrimination: international instruments

## ICCPR (1966)

**Art. 2:** Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

**Art. 26:** All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

## ECHR (1950)

**Art. 14:** The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

**Protocol 12:** The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.



# Prohibition of discrimination: international instruments

## ICESCR (1966)

**Art. 2:** The States Parties to the present Covenant undertake to guarantee that the rights enunciated in the present Covenant will be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

## ESCh (Revised) (1996)

**Article E:** The enjoyment of the rights set forth in this Charter shall be secured without discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national extraction or social origin, health, association with a national minority, birth or other status.

# Special non-discrimination treaties

Universal	Regional
1965 International Convention on the Elimination of All Forms of Racial Discrimination (CERD);	1992 European Charter for Regional or Minority Languages (ECRML);
1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW);	1995 Framework Convention for the Protection of National Minorities (EFCNM);
1989 Convention on the Rights of the Child (CRC);	1996 European Convention on the Exercise of Children's Rights;
1990 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families;	2011 Council of Europe Convention on preventing and combating violence against women and domestic violence;
2006 Convention on the Rights of Persons with Disabilities	EU anti-discrimination directives (2000/43/EC; 2000/78/EC; 2006/54/EC; 2004/113/EC).



# Discrimination

Discrimination should be understood to imply any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on equal footing, of all rights and freedoms

# Elements of Discrimination

Stipulates a  
difference in  
treatment

Has a certain  
effect

Is based on  
a certain  
prohibited  
ground



# Types of discrimination

## Direct discrimination

Less favourable or detrimental treatment of an individual or group of individuals on the basis of a prohibited characteristic or ground such as race, sex, disability etc.

## Indirect discrimination

Occurs when a practice, rule, requirement or condition is neutral on its face but impacts disproportionately upon particular groups, unless that is justified

# Positive discrimination or affirmative measures (also known as 'special measures')

Proactive measures taken to remedy the effects of past and present discrimination by instituting preferences that favour members of previously disadvantaged societal groups.

Must have an 'objective and reasonable justification':

- (i) pursue a legitimate aim;
- (ii) there must be a reasonable relationship of proportionality between the aim sought to be realised and the means employed to achieve it.



# Comparison of provisions on equality

	Open-ended or Specified Group	Free-Standing or Dependent	Direct and Indirect	Positive Action	Group Rights
ICCPR	<b>Open-ended</b> 26 and 2(1): 'or other status' 3: Special provision prohibiting sex discrimination	<b>Free-standing</b> 26: 'equal protection before the law' 2(1): 'in the present covenant'	<b>Both</b> HRC G.C. 18(7): 'purpose or effect'	<b>Yes</b> HRC G.C. 18(10): 'equality sometimes requires States to take affirmative action.'	<b>Yes</b> 1: Peoples' right to self-determination and means of subsistence
ICESCR	<b>Open-ended</b> 2(2): 'or other status' 3: sex discrimination 2(3): non-nationals (distinction allowed)	<b>Dependent</b> 2(2): 'rights enunciated in the present convention'	[See ICCPR]	<b>N/A</b>	<b>Yes</b> 1: Peoples' right to self-determination and means of subsistence
CERD	<b>Specified</b> 1(1): 'race, colour, descent, or national or ethnic origin'	<b>Free-standing</b> 1(1): 'any other field' 5: 'equality before the law'	<b>Both</b> 1(1): 'purpose or effect' 2(c): 'which have the effect'	<b>Yes</b> 1(4) and 2(2): Special measures do not constitute discrimination	<b>N/A</b>
CEDAW	<b>Specified</b> 1(1): 'discrimination against women'	<b>Free-standing</b> 1(1): 'or any other field'	<b>Both</b> 1(1): 'purpose or effect'	<b>Yes</b> 4: Promotes positive action	<b>N/A</b>
CRC	<b>Open-ended, but applies only to children</b> 2(1): All children, regardless of 'other status'	<b>Dependent</b> 2(1): 'rights set forth in the present Convention'	<b>Both</b> 2(1): 'discrimination of any kind'	<b>N/A</b>	<b>Yes</b> 30: Indigenous/ minority children have right to own community, culture, religion, and language
CRPD	<b>Open-ended, but applies only to persons with disabilities and their families</b> 2(1): All persons with disabilities, regardless of 'other status'	<b>Freestanding</b> 5(1) Equal before and under the law	<b>Both</b>	<b>Yes</b>	<b>N/A</b>

# Comparison of provisions on equality

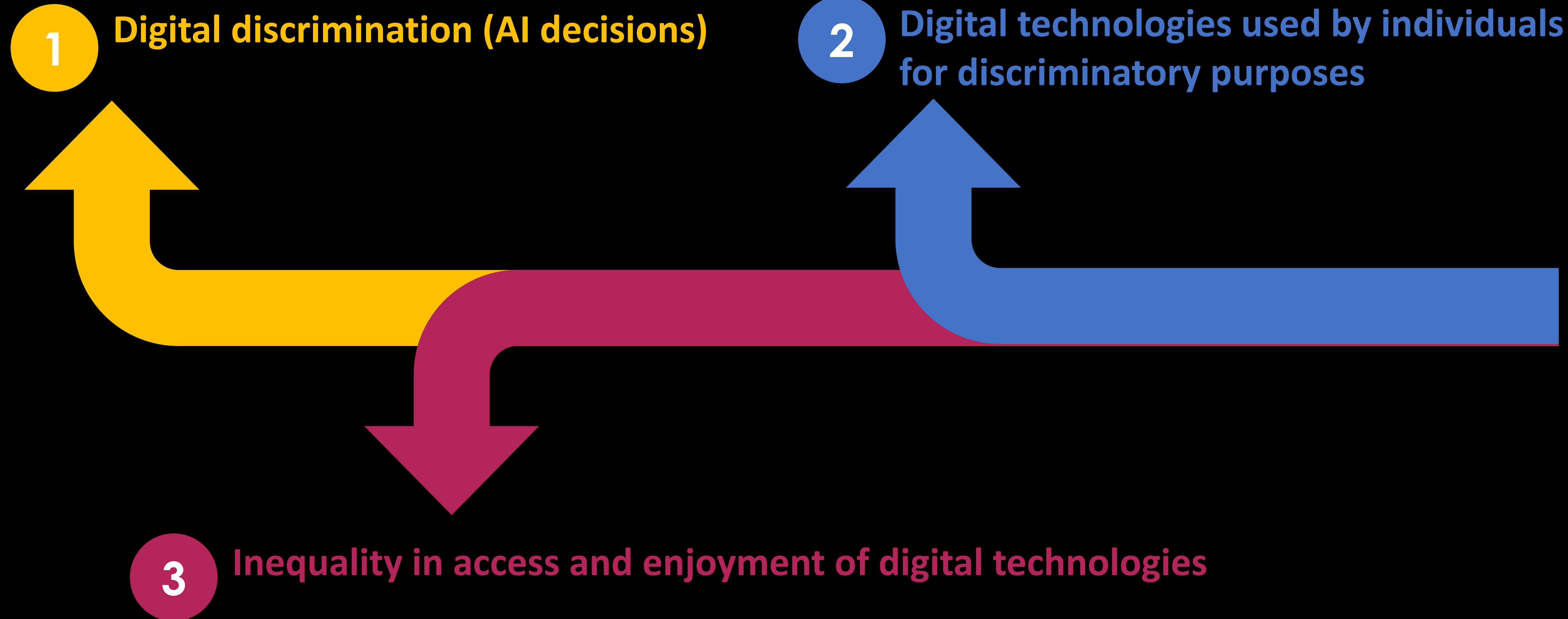
<b>ECHR European Convention</b>	<b>Open-ended</b> 14(1): 'or other status'	<b>Dependent</b> 14(1): 'set forth in this convention' (Compare Protocol No. 12: 'any right set forth by law')	<b>Both</b> Protection against indirect discrimination clarified in case law: see <i>Hugh Jordan v the United Kingdom</i> etc.	<b>Yes</b> Positive action permissible clarified in case law. See, for example, <i>Belgian Linguistics</i> ; and <i>Thlimmenos v Greece</i> .	<b>N/A</b>
<b>EU EC Treaty &amp; EC Directives</b>	<b>Specified</b> EC Treaty 141 & 39: sex and nationality Framework Dir. 1: 'religion or belief, disability, age, or sexual orientation' Race Dir. 1: 'racial or ethnic origin' Revised Equal Treatment Directive: sex/gender	<b>Dependent</b> EC Treaty 141(1); 39(2): work conditions, employment, and remuneration. Framework, Race, and Revised Equal Treatment Directives: employment and occupation, vocational training, etc.	<b>Both</b> Framework, and Race Directives, 2(2)(b): 'indirect discrimination' Revised Equal Treatment Directive, 1: 'either directly or indirectly'	<b>Yes</b> TA 141(4): positive action regarding sex acceptable Framework Dir. 7(1); Race Dir. 5: accepts positive action measures. Also Equal Treatment Directive: 4	<b>N/A</b>
<b>AfCHPR African Charter</b>	<b>Open-ended</b> 2: 'or other status'	<b>Free-standing</b> 3: 'equal protection of the law and equality before the law' 2: 'guaranteed in the present Charter' [Dependent]	<b>(Direct)</b> [unclear from the case law whether indirect discrimination covered]	[Not addressed in the case law]	<b>Yes</b> 19: 'Nothing shall justify the domination of a people by another.' 22: 'peoples shall have the right to their economic, social and cultural development'
<b>AmCHR American Convention</b>	<b>Open-ended</b> 1(1): 'or other social conditions'	<b>Free-standing</b> 24: 'equal protection of the law' - as interpreted by Advisory Opinion No. 4. 1(1): 'recognised herein'	<b>Both</b> See <i>Advisory Opinion OC-18/03</i> at paragraph 103.	<b>Yes</b> See <i>Advisory Opinion OC-18/03</i> at paragraph 104.	



# Burden of proof: ECHR

- The burden of proof in discrimination cases is split.
- An applicant must first show that the complaint falls within the ambit of one of the substantive Convention rights and that he/she has been treated differently from a person in a comparable position with respect to that right.
- The burden then shifts onto the State to prove that the difference in treatment was lawful.

# Discrimination and emerging digital technologies



## Digital discrimination

Digital discrimination is a form of discrimination in which automated decisions taken by algorithms, increasingly based on Artificial Intelligence techniques like Machine Learning, treat users unfairly, unethically or just differently based on their personal data such as income, education, gender, age, ethnicity, religion.

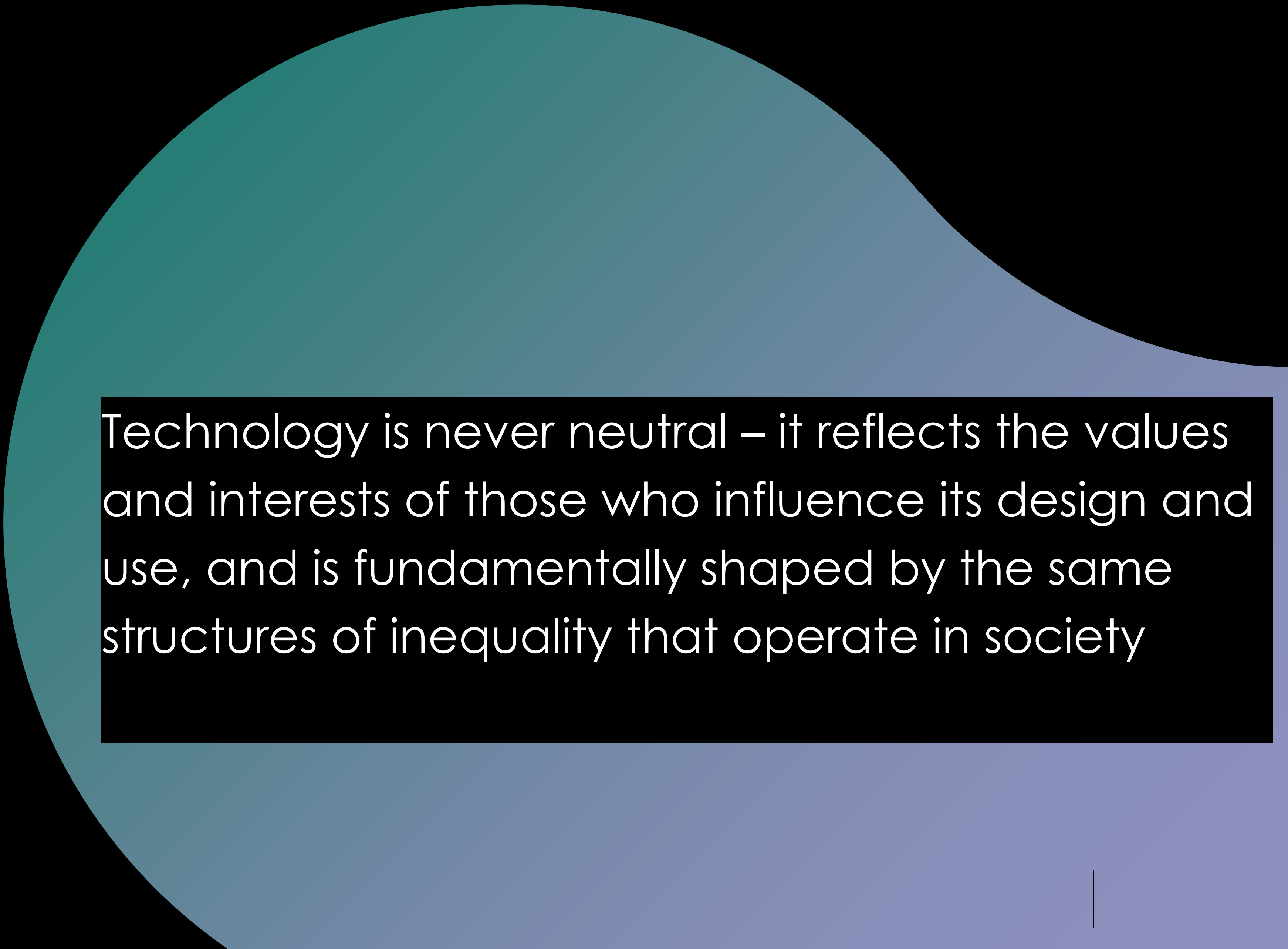


# Digital discrimination

Digital discrimination is becoming a serious problem, as more and more tasks are delegated to computers, mobile devices, and autonomous system.

From the jobs we apply for, to the products we buy, to the news we read and to the persons we date, many sensitive decisions are increasingly delegated to or, at least, influenced by those systems

Machine learning algorithms have the potential to discriminate more consistently and systematically and at a larger scale than traditional non-digital discriminatory practices.



Technology is never neutral – it reflects the values and interests of those who influence its design and use, and is fundamentally shaped by the same structures of inequality that operate in society

# Examples of digital discrimination

**Gender:** Google showed males ads encouraging the use of coaching services for high paying jobs more frequently than females, which may lead to discriminate women and to increase the gender pay gap a slight under-representation of women (when compared to actual gender distributions of the different professions considered in the study) and that the female gender for a given profession was usually depicted less professionally. Findings suggest that women are well covered by Wikipedia, however there are significant differences in the way in which they are portrayed. Women pages contain more information about their personal lives and their pages are less central in the network of pages when compared to male pages

**Race or ethnicity:** advertisements suggestive of arrest records appear more often with searches of black-sounding names than white-sounding names, regardless of the existence of arrest records for those names. A 2019 review of 189 facial recognition algorithms from 99 developers around the world found that “many of these algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics.

**Income, Location & Lifestyle.** Aspects related to income, location or lifestyle may also lead to digital discrimination. A very clear example of intentional direct discrimination is the current practice of targeting low-income population with high-interest loans



# Inequalities in access to and enjoyment of the benefits of emerging digital technologies track

Geopolitical inequalities at the international level (In Africa, 22 per cent of individuals use the Internet, compared with 80 per cent in Europe)



Patterns of racial, ethnic and gendered inequality within individual countries (USA: 82% of whites report owning a desktop or laptop computer, only 58% of blacks and 57% of Hispanics do)

# Cybercrime and human rights



## Council of Europe Convention on Cybercrime (Budapest convention)

The Budapest Convention is more than a legal document; **it is a framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation** in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention.

Any country may make use of the Budapest Convention as **a guideline, check list or model law**. Furthermore, becoming a Party to this treaty entails additional advantages

The treaty's objectives are three-fold: 1) harmonizing national laws related to cyber-related crime; 2) supporting the investigation of these crimes; and 3) increasing international cooperation in the fight against cybercrime



## **Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence**

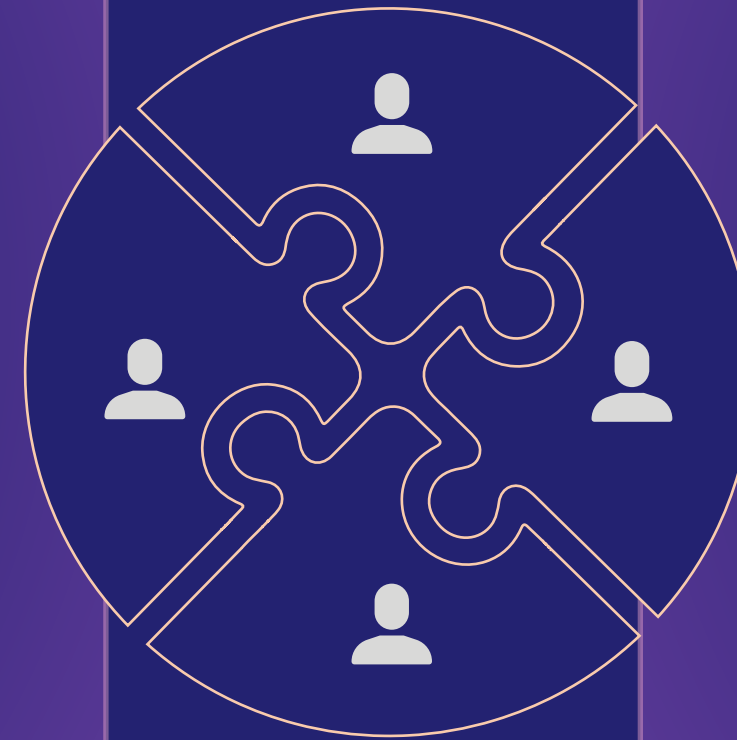
On 17 November 2021, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions. As a response, the Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards. The text will be opened for signature in Strasbourg on 12 May 2022.

# Cybercrime

Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime. Cybercrime differs from traditional crime in that it "knows no physical or geographic boundaries" and can be conducted with less effort, greater ease, and at greater speed than traditional crime (although this depends on the type of cybercrime and type of crime it is being compared to)

# Types of cybercrimes

*Cyber-dependent* crimes  
(i.e., "any crime that can only be committed using computers, computer networks or other forms of information communication technology)



*Cyber-enabled* crimes  
(i.e., traditional crimes facilitated by the Internet and digital technologies)

The key distinction between these categories of cybercrime is the role of ICT in the offence - whether it is the target of the offence or part of the *modus operandi* (or M.O.; i.e., method of operation) of the offender



# Cybercrime

Cybercrime can be perpetrated by individuals, groups, businesses, and nation-states. While these actors may use similar tactics (e.g., using malicious software) and attack similar targets (e.g., a computer system), they have different motives and intent for committing cybercrimes

# Cybercrime and human rights

Several national cybercrime laws in various parts of the world already unduly restrict rights and are being used to persecute journalists, human rights defenders, technologists, opposition politicians, lawyers, religious reformers, and artists. Any effort to address cybercrime needs to reinforce, not undermine, freedom of expression and other human rights.

In recent years, there has been a surge in cybercrime laws around the world, some of which are overly broad and criminalize online expression, association, and assembly. cybercrime laws are “in some instances misused to target human rights defenders or have hindered their work and endangered their safety in a manner contrary to international law.”

# Cybersecurity and human rights





# Cybersecurity: definition

European Union: “safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure”

International Telecommunications Union: “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets”

Freedom Online Coalition’s cybersecurity Working Group “An Internet Free and Secure”: “Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to preserve the security of persons both online and offline.”

## Cybersecurity: definition

The Internet Society (ISOC) has pointed that cybersecurity is “a catchword” that is “frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and “solutions” ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity.”

## Cybersecurity and human rights: some examples of interaction

- Processing of personal data for cybersecurity purposes
- Monitoring communications
- Creating conditions for surveillance of communication networks
- Content filtering, blocking, removal

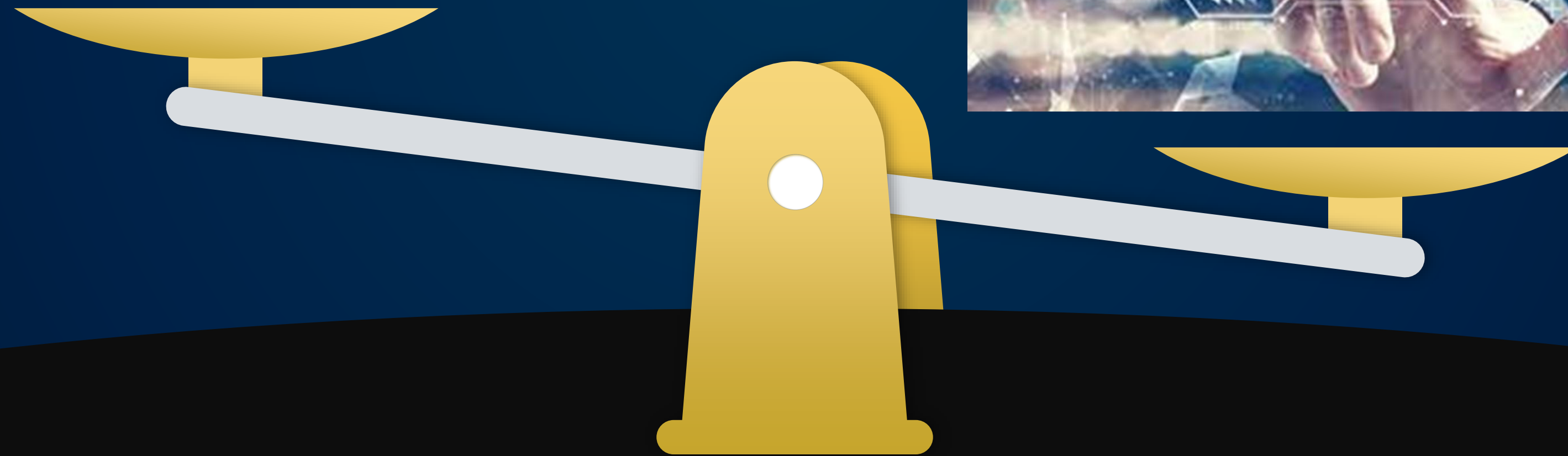


# Fair balance?

Human rights

v.

Cybersecurity



# Restrictions

1

## Legality

**In accordance with the law**

- Prescribed by national law
- Law must be adequately accessible
- Law must be clear and definite

2

## Legitimacy

**Legitime aims**

- national security
- Territorial integrity or public safety
- prevention of disorder or crime
- protection of health or morals
- protection of the reputation or rights of others
- preventing the disclosure of information received in confidence
- maintaining the authority and impartiality of the judiciary

3

## Proportionality

**Necessary in a democratic society**

- correspond to a pressing social need
- proportional to the legitimate aim pursued
- justified by relevant and sufficient reasons



# PROBLEMS FACED BY CURRENT CYBERSECURITY HUMAN RIGHTS

The expansion of government activities under the banner of cybersecurity, with little clarity as to what is being done and to what end



Difficulty of making technical issues accessible to a broader audience



The complex form of laws and policies related to the internet



Lack of transparency around the use by government of offensive cyber capabilities



Lack of transparency around government agencies that monitor and control internet usage



Change in nature of technologies, lack of public understanding, and digital literacy





# Children rights in the digital environment



 <p>1</p> <p>DEFINITION OF A CHILD</p>	 <p>2</p> <p>NO DISCRIMINATION</p>	 <p>3</p> <p>BEST INTERESTS OF THE CHILD</p>	 <p>4</p> <p>MAKING RIGHTS REAL</p>	 <p>5</p> <p>FAMILY GUIDANCE AS CHILDREN DEVELOP</p>	 <p>6</p> <p>LIFE, SURVIVAL AND DEVELOPMENT</p>	 <p>7</p> <p>NAME AND NATIONALITY</p>
 <p>8</p> <p>IDENTITY</p>	 <p>9</p> <p>KEEPING FAMILIES TOGETHER</p>	 <p>10</p> <p>CONTACT WITH PARENTS ACROSS COUNTRIES</p>	 <p>11</p> <p>PROTECTION FROM KIDNAPPING</p>	 <p>12</p> <p>RESPECT FOR CHILDREN'S VIEWS</p>	 <p>13</p> <p>SHARING THOUGHTS FREELY</p>	 <p>14</p> <p>FREEDOM OF THOUGHT AND RELIGION</p>
 <p>15</p> <p>SETTING UP OR JOINING GROUPS</p>	 <p>16</p> <p>PROTECTION OF PRIVACY</p>	 <p>17</p> <p>ACCESS TO INFORMATION</p>	 <p>18</p> <p>RESPONSIBILITY OF PARENTS</p>	 <p>19</p> <p>PROTECTION FROM VIOLENCE</p>	 <p>20</p> <p>CHILDREN WITHOUT FAMILIES</p>	 <p>21</p> <p>CHILDREN WHO ARE ADOPTED</p>
 <p>22</p> <p>REFUGEE CHILDREN</p>	 <p>23</p> <p>CHILDREN WITH DISABILITIES</p>	 <p>24</p> <p>HEALTH, WATER, FOOD, ENVIRONMENT</p>	 <p>25</p> <p>REVIEW OF A CHILD'S PLACEMENT</p>	 <p>26</p> <p>SOCIAL AND ECONOMIC HELP</p>	 <p>27</p> <p>FOOD, CLOTHING, A SAFE HOME</p>	 <p>28</p> <p>ACCESS TO EDUCATION</p>
 <p>29</p> <p>AIMS OF EDUCATION</p>	 <p>30</p> <p>MINORITY CULTURE, LANGUAGE AND RELIGION</p>	 <p>31</p> <p>REST, PLAY, CULTURE, ARTS</p>	 <p>32</p> <p>PROTECTION FROM HARMFUL WORK</p>	 <p>33</p> <p>PROTECTION FROM HARMFUL DRUGS</p>	 <p>34</p> <p>PROTECTION FROM SEXUAL ABUSE</p>	 <p>35</p> <p>PREVENTION OF SALE AND TRAFFICKING</p>
 <p>36</p> <p>PROTECTION FROM EXPLOITATION</p>	 <p>37</p> <p>CHILDREN IN DETENTION</p>	 <p>38</p> <p>PROTECTION IN WAR</p>	 <p>39</p> <p>RECOVERY AND REINTEGRATION</p>	 <p>40</p> <p>CHILDREN WHO BREAK THE LAW</p>	 <p>41</p> <p>BEST LAW FOR CHILDREN APPLIES</p>	 <p>42</p> <p>EVERYONE MUST KNOW CHILDREN'S RIGHTS</p>

43-54



HOW THE CONVENTION WORKS

# CONVENTION ON THE RIGHTS OF THE CHILD

## **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)**

Contains provisions criminalising the use of new technologies – the Internet in particular – to sexually harm or abuse children. The convention represents major progress towards preventing sexual offences against children, prosecuting the perpetrators and protecting their victims.

It is the only international treaty to make sexual abuse a criminal offence, with criminal penalties for:

- those who recruit children into prostitution and those who have recourse to them;
- the production, supply, distribution and possession of child pornography and online access to it;
- soliciting children on chat rooms or online game sites for sexual purposes.

As a preventive measure, the convention recommends that primary and secondary school children be informed of the risks of Internet use



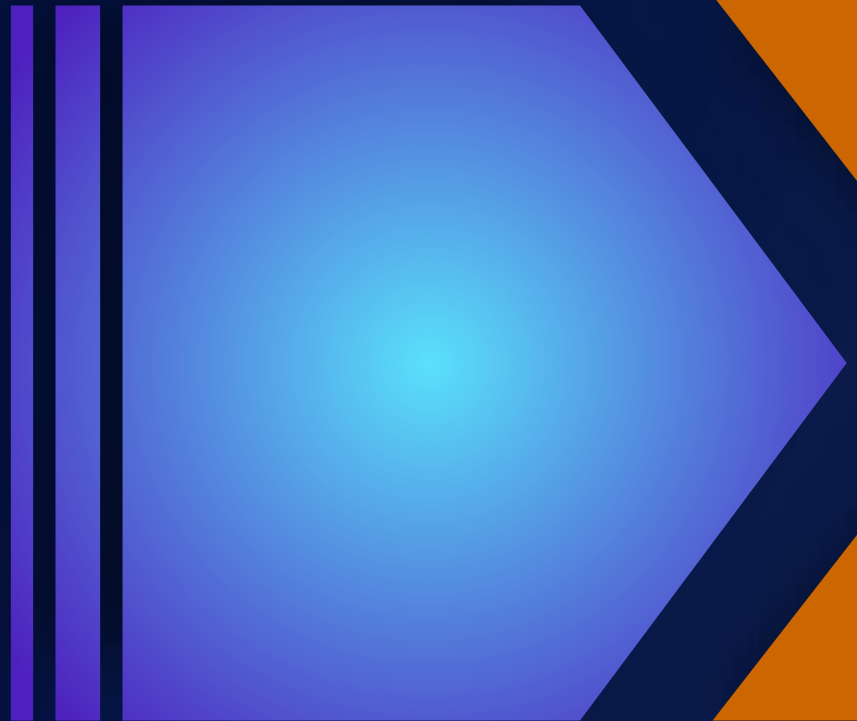
## OECD Recommendation on Children in the Digital Environment (2021)

The Recommendation recognises both the integral role of the digital environment in the daily lives of our children and the urgent need to support policy makers and other stakeholders to create safe, beneficial and equitable conditions for all children. This approach focuses on bringing legal and policy responses up to date with technological advancement, developing a strong evidence-base, and building coherent policy responses. The Recommendation aims to help countries to find a balance between protecting children from online risks, and promoting the opportunities and benefits that the digital world provides. The Recommendation sets out principles for promoting a safe and beneficial digital environment for children, recommendations on overarching policy frameworks, and highlights the importance of international co-operation.

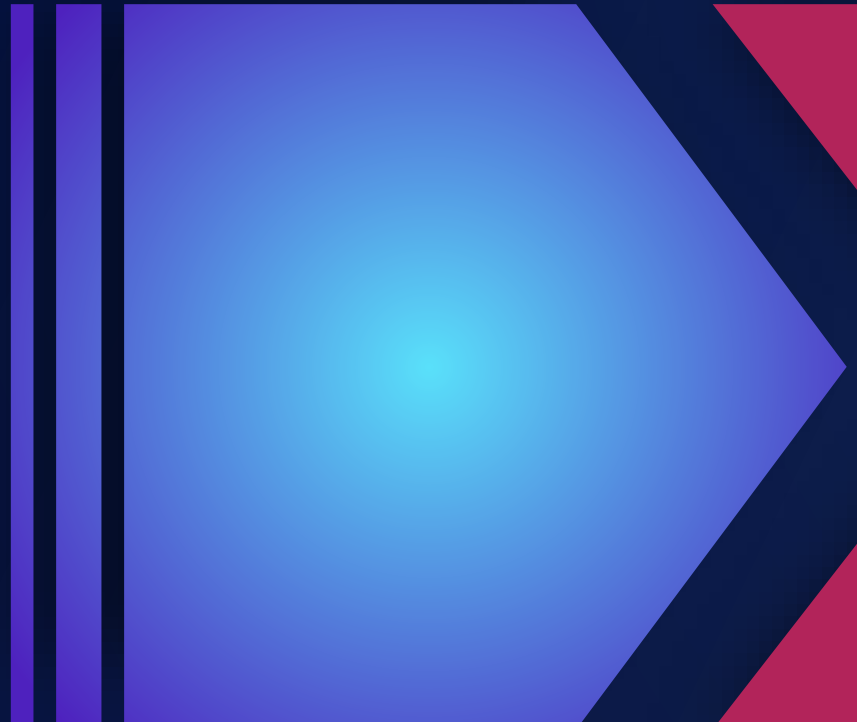
## Best interests of the child

In all actions concerning children in the digital environment, the best interests of the child shall be a primary consideration. In assessing the best interests of a child, States should make every effort to balance, and wherever possible, reconcile a child's right to protection with other rights, in particular the right to freedom of expression and information as well as participation rights.

# Children online



More than a third of young people in 30 countries report being cyberbullied, with 1 in 5 skipping school because of it.



Some 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online.



# Children online: risks

Cyberbullying and other forms of peer-to-peer violence can affect young people each time they log in to social media or instant messaging platforms. When browsing the internet, children may be exposed to hate speech and violent content – including messages that incite self-harm and even suicide.

Children can also be put at risk when tech companies breach their privacy to collect data for marketing purposes. Child-targeted marketing through apps – and the excessive screen time it often results in – can compromise a child's healthy development.

Most alarming is the threat of online sexual exploitation and abuse. It has never been easier for child sex offenders to contact their potential victims, share imagery and encourage others to commit offences. Children may be victimized through the production, distribution and consumption of sexual abuse material, or they may be groomed for sexual exploitation, with abusers attempting to meet them in person or exhort them for explicit content.

# Children online: risks

Risks for Children in the Digital Environment				
Risk Categories	Content Risks	Conduct Risks	Contact Risks	Consumer Risks
Cross-cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

# Children online: content risks

Hateful content can take the form of pictures, words, videos, games, symbols and even songs. It can be motivated, for instance, by the victim's religion, race, gender, disability, sexual orientation or gender identity.

Children can also be troubled by a wide variety of harmful content, such as online scams, pornographic pop-up advertisements, unpleasant or scary news or pictures. Violent and pornographic content can cause children shock and disgust

Content that is illegal to publish (i.e. illegal content) can expose children to concepts that they are unable to manage and can also breach cultural and social norms. For example, images or videos of child sexual abuse, content that advocates terrorist acts, or promotes, instructs or incites crime or violence is considered illegal in many countries

Children need to be educated about disinformation so that they are able to distinguish between what is fact and what is false or a misrepresentation in the digital environment. This is an especially key skill given that children can have different interpretations of what makes a news outlet credible and they mostly obtain news and information from social media platforms, which can be unreliable



## Children online: conduct risks

This is a risk where children are actors in a peer-to-peer exchange, including when their own conduct can make them vulnerable (for instance in the case of sexting, or cyberbullying). Such risks manifestations not only pose a risk towards those children who are on the receiving end of such behaviour in the digital environment, but also to those whose behaviour created the risk

## Children online: cyberbullying

A lack of agreement across policy actors and research as to what actually constitutes cyberbullying has resulted in countries addressing this concern in different ways – in many cases by criminal justice responses. However, where children are the perpetrators, a criminal justice response can be highly controversial and disproportionate as it can lead to the criminalisation of children unaware of the impact of their actions.

## Children online: sexting

Sexting, the exchange of sexual messages, on the other hand, provides an example of user-generated problematic behaviour. It can cause a multitude of problems (both social and legal) for the creator(s) of the content. Whilst, intuitively it may seem that sexting would emerge as a risk only if an image is shared without the subject's consent, when minors engage in sexting (even in those cases when their 'sext' is shared consensually), they may be self-producing child pornography material that can quickly spread and remain in the digital environment permanently. Sexting not only has implications on a child's privacy, health and wellbeing, but there is also a significant risk that a child could be criminalised as a result of 'self-producing' child pornographic material



# Effective remedies for restriction or violation of rights online



# Effective remedies

Article 13 of the ECHR guarantees the availability, at the national level, of a remedy to enforce the substance of ECHR rights and freedoms in whatever form they might happen to be secured in the domestic legal order

There should be a national authority tasked with deciding on allegations of violations of the rights guaranteed in the ECHR

States, as part of their positive obligations to protect individuals against violations of human rights by private companies, should take appropriate steps to ensure that when such violations occur those affected have access to judicial and non-judicial mechanisms

Internet users should be offered clear and transparent information regarding the means of redress available to them



# SUMMARY





**“the same rights that people have offline  
must also be protected online”**

2012 UN Human Rights Council  
Resolution

# Digitalization and human rights

Hate speech

Freedom of speech

Intrusion of privacy

Accessibility

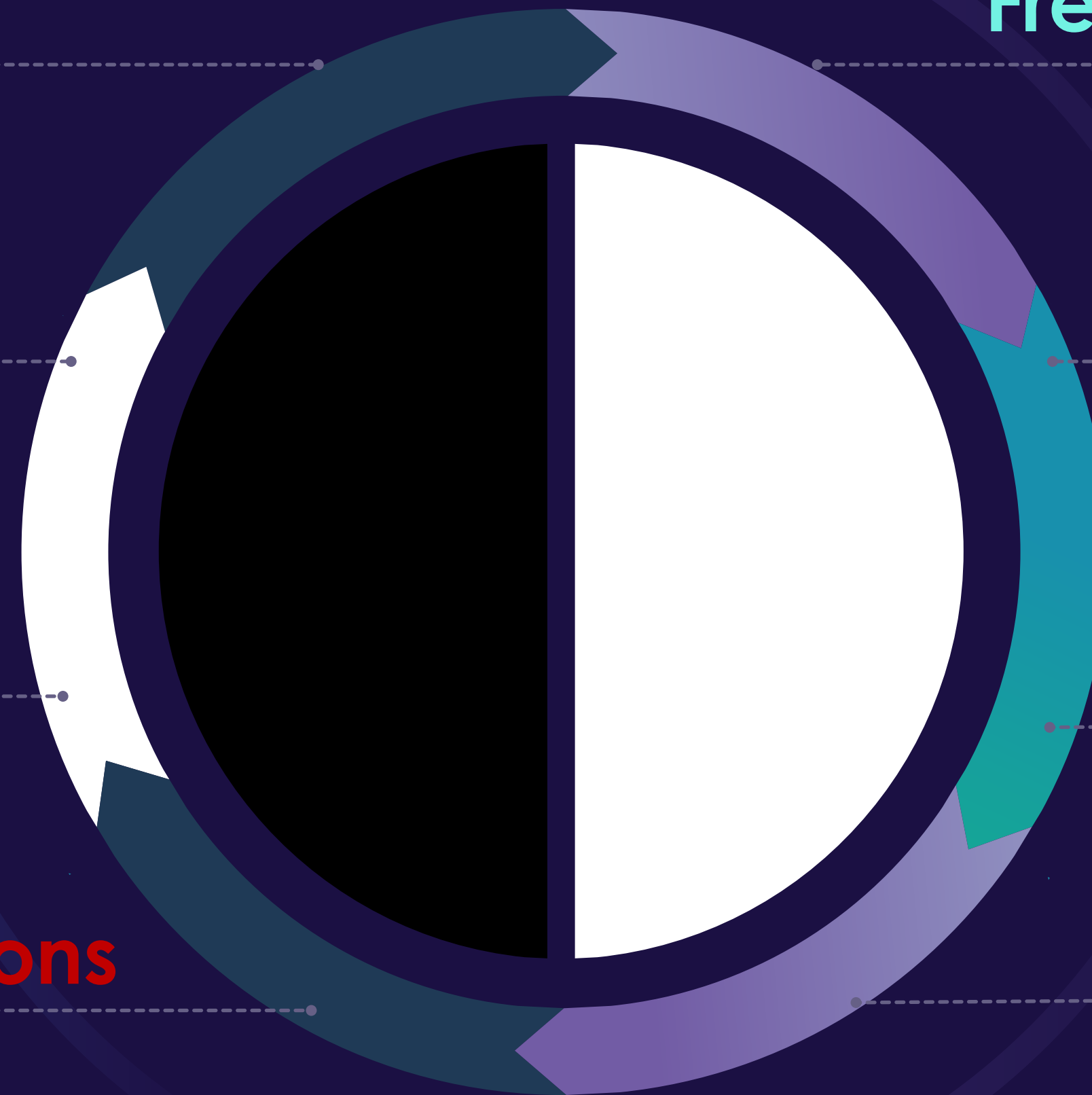
Propaganda, disinformation

Promotion of democracy

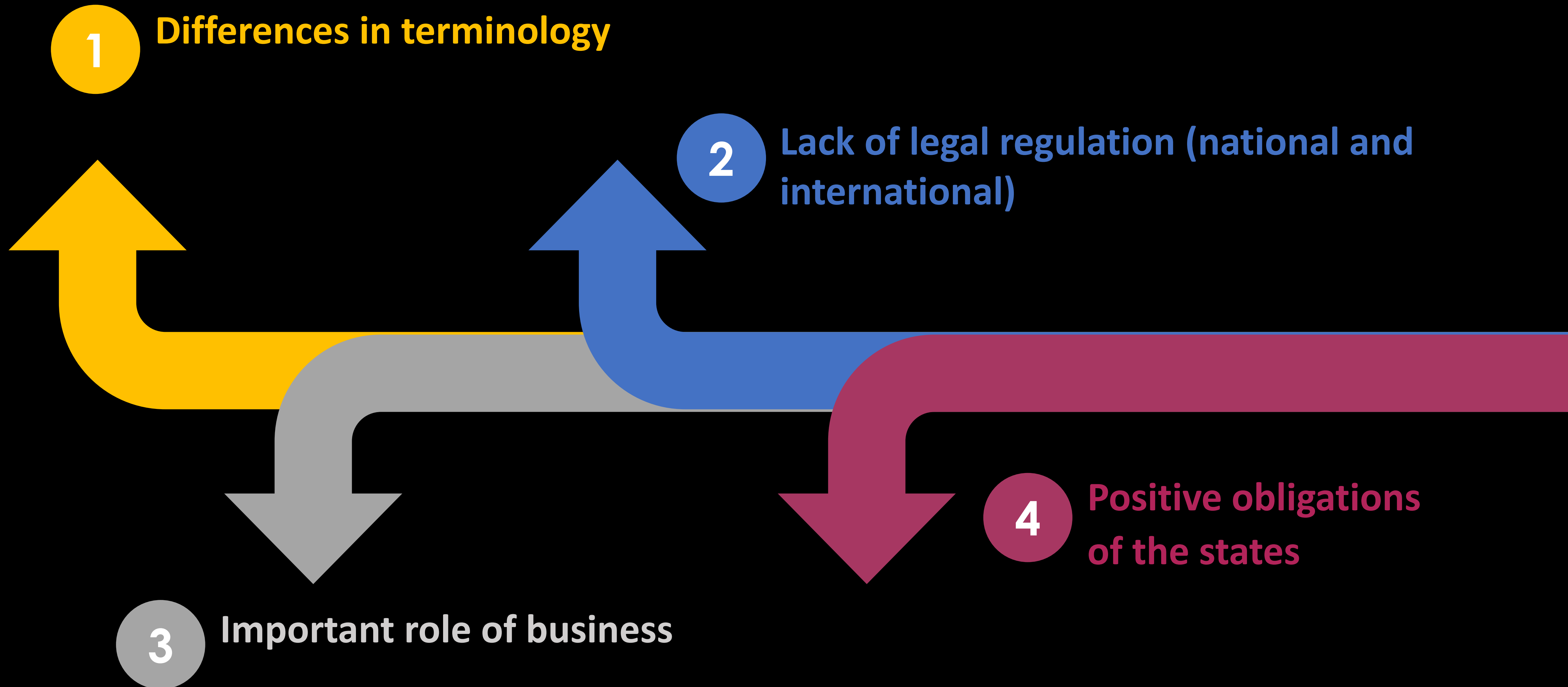
Influence on elections

Security


Digital technologies provide new means to exercise human rights,  
but they are too often also used to violate them



# Challenges







**“At its best, the digital revolution will empower, connect, inform and save lives. At its worst, it will disempower, disconnect, misinform and cost lives.”**

Michelle Bachelet, UN High Commissioner for  
Human Rights



**THANK YOU**  
**QUESTIONS?**

**Evaluation of the Course**

**Contacts: [dgailiute@mruni.eu](mailto:dgailiute@mruni.eu)**