Politecnico di Torino

Computer Forensics
Class 2024/2025

UN Resolution
26 May 2021 and 19 August 2024

Background and objectives of the resolution

Context and Objectives of the Resolution

🔎The primary objective of the resolution is to initiate the drafting of a global treaty to combat cybercrime through multilateral negotiations. Even the title "Countering the use of information and communications technologies for criminal purposes" represents a significant step towards the development of an international convention on cybercrime, aiming to implement concrete measures to fight this type of crime

🔎The resolution establishes a specific Committee tasked with drafting a comprehensive convention, which is expected to operate transparently and involve a wide range of stakeholders, including developing countries, intergovernmental organizations, and experts in the field.

Impact on international cybersecurity policies and practices

UN resolution May 26, 2021 & Cybersecurity policies

🔎The adoption of this resolution could have a significant impact on international cybersecurity policies, promoting greater cooperation and harmonization among states. Creating an international cybercrime treaty means establishing **shared minimum standards,** which could lead to a more unified regulatory framework and improve investigative cooperation across different jurisdictions

🔎The adoption also required **multiple amendments and compromises** to ensure broad support, which highlights the need to balance national and supranational interests, ensuring inclusivity and transparency

UN resolution May 26, 2021 - implications and risks on cybersecurity

🔎Human Rights and Privacy Risks

One of the central issues discussed in the UN report is the need to balance cybersecurity measures with the protection of human rights, including privacy and data protection.

While there is consensus on the importance of cybersecurity, the UN GGE report underscores the risk of overreach, where measures to enhance cybersecurity could infringe on civil liberties if not carefully regulated

UN resolution May 26, 2021 - implications and risks on cybersecurity

🔎Emerging Threats and the Role of Supply Chain Integrity

The report also emphasizes the growing risks posed by vulnerabilities in global supply chains, especially in the ICT sector.

These vulnerabilities could be exploited to carry out large-scale attacks or espionage, highlighting the need for states to secure their digital infrastructures and cooperate in sharing information about emerging threats

Future Legal Framework for Cybersecurity

- 🔎Cybersecurity policy makers are required to introduce strict cybersecurity measures to protect data during investigations

- 🔎Legislative provisions should be issued allowing for periodic review and updates to cybersecurity practices, ensuring that they keep pace with evolving digital threats.

Analysis of the resolution's key components and their legal implications

Key components

🔎Ad Hoc Committee

The resolution establishes an Ad Hoc Committee to draft a global convention on cybercrime. This committee must convene at least six times, with each session lasting 10 days, starting in January 2022, and it **must present the treaty**.

Its substantive decisions must be made, when consensus cannot be reached, by a two-thirds majority.

International law issues

🔎Cyber Sovereignty and Legal Boundaries

The concept of cyber sovereignty poses a significant legal dilemma. Countries like China and Russia advocate for state control over cyberspace, which can conflict with international norms on internet freedom and the open nature of the global internet.

The UN resolution attempts to address these tensions, but the broader legal debate on how much control states should have over their digital borders remains unresolved. This issue touches on the broader governance of cyberspace, where states must balance sovereignty with global cooperation

International law issues

🔎Public-Private Cooperation and Liability

Legal frameworks also need to account for the growing role of private companies in cybersecurity.

The resolution encourages greater collaboration between states and private actors, such as internet service providers and cybersecurity firms, to combat cyber threats. However, this raises legal questions about the responsibility and liability of these companies, especially when they are involved in preventing or responding to cyberattacks

International law issues

Article 22

Jurisdiction outlines the conditions under which State Parties must establish their jurisdiction over offences defined by the Convention. Here is a detailed summary:

Territorial Jurisdiction:

States must ensure they have jurisdiction over offences committed within their territory or on a vessel or aircraft registered under their laws.

Extended Jurisdiction:

States may also establish jurisdiction over offences that:

- Are committed against their nationals.
- Are committed by one of their nationals or a stateless person habitually residing in their territory.
- Are committed outside their territory with the intent of carrying out an offence within their territory as specified in Article 17 of the Convention.
- Are committed against the State itself.

International law issues

Jurisdiction and Non-extradition:

States must establish jurisdiction if the alleged offender is present in their territory and is not extradited solely due to their nationality.
Jurisdiction for Other Non-extradition Cases:

States may take measures to establish jurisdiction when the alleged offender is present in their territory and is not extradited for reasons other than nationality.

Coordination Among States:

When a State exercising jurisdiction becomes aware that other States are conducting investigations or proceedings for the same offence, competent authorities should consult to coordinate their actions.

Compatibility with International Law:

The Article affirms that this Convention does not preclude a State Party from exercising other forms of criminal jurisdiction as allowed under its domestic law.

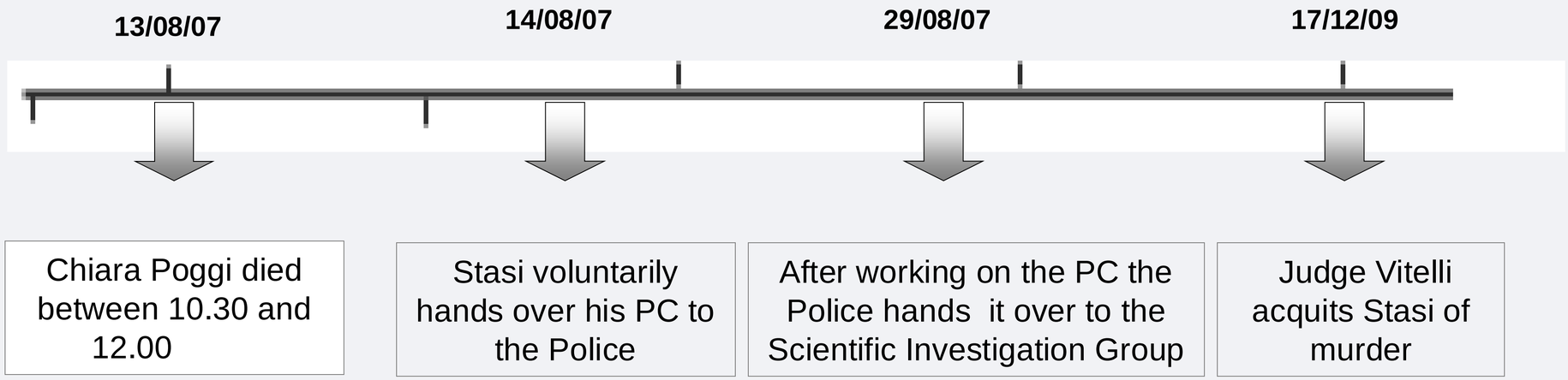
Garlasco Case

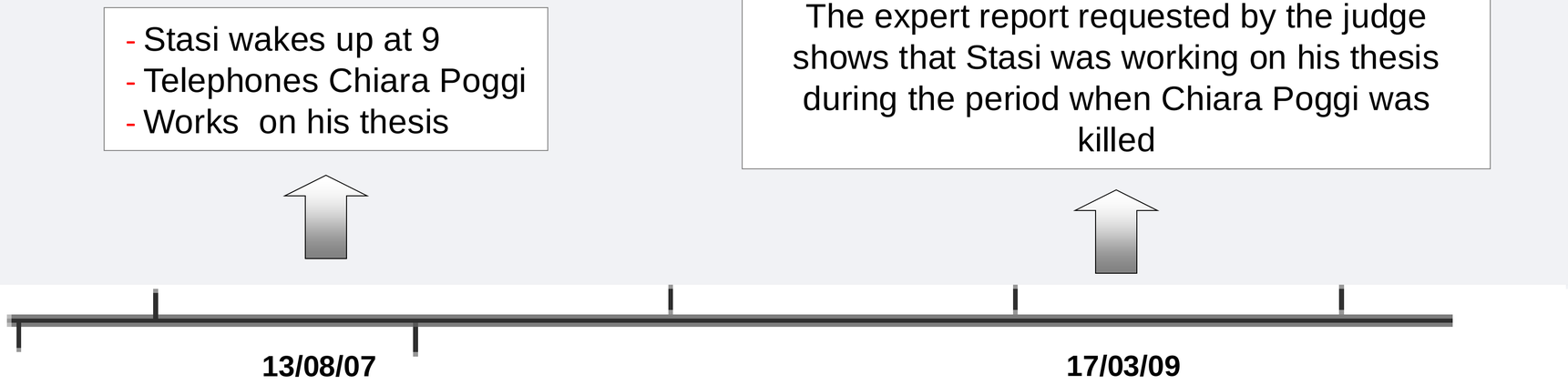
Italian Case Law on Digital Forensics

Digital evidence could be altered and can contain countless pieces of information. The “Garlasco” case is a clear example of this.

Alberto Stasi was acquitted of murder of his girlfriend, Chiara Poggi, by the Court of first Instance In December 2009 and the judgement was confirmed in the Appeal court in December 2011.

The “Garlasco” case: the “IT alibi”





The Internet of the Human Body: Towards a habeas data?

“If your internet thermostat's pinging servers all day, will the cops think you're a weed farm? Or just a hot yoga gym?”

Jonathan Zittrain

“Sure, encrypt your email – while your shiny IoT toothbrush spies on you”

Susan Landau

Connie Debate Case: Fitbit

"As people continue to provide more and more personal information through technology, they have to understand we are obligated to find the best evidence, and this technology has become a part of that."

Detective Christopher Jones - East Lampeter Township Police Department in Pennsylvania

"We are entering an era of sensorveillance. People are just waking up to the fact that their smart devices are going to snitch on them and that they are going to reveal intimate details about their lives they did not intend law enforcement to have"

Andrew Ferguson, a University of the District of Columbia law professor,

James Bate Case: Amazon Echo

“The Amazon Echo device is constantly listening for the 'wake' command of 'Alexa' or 'Amazon,' and records any command, inquiry, or verbal gesture given after that point”

Search Warrant

“The allegation that the Echo is possibly recording at all times without the wake word being issued is incorrect”

Answer of an Amazon Representative

Ross Compton Case: Pacemaker

“Americans shouldn't have to make a choice between health and privacy. Compelling citizens to turn over protected health data to law enforcement erodes those rights.”

Electronic Frontier Foundation Attorney Stephanie Lacambra

“There is a lot of other information about things that may characterize the inside of my body that I would much prefer to keep private rather than how my heart is beating. It is just not that big of a deal”

Judge Charles Pater

Facial Recognition Biometric Border

“Face Recognition has a great potential for expansion and misuse: for example, you can subject thousands of people to face recognition when they’re walking down the sidewalk without their knowledge”

Senior Policy Analyst, ACLU - Jay Stanley,

“U.S. Customs and Border Protection says it will delete the live photos captured at the gate within 14 days for citizens, and that it only uses them to verify identity by comparing them with the database photos”

CBP Privacy Impact Assessment

3 categories of law enforcement activity

Situations involving officers observing an ongoing crime

Situations involving officers investigating a past crime

Situations involving officers predicting a future crime

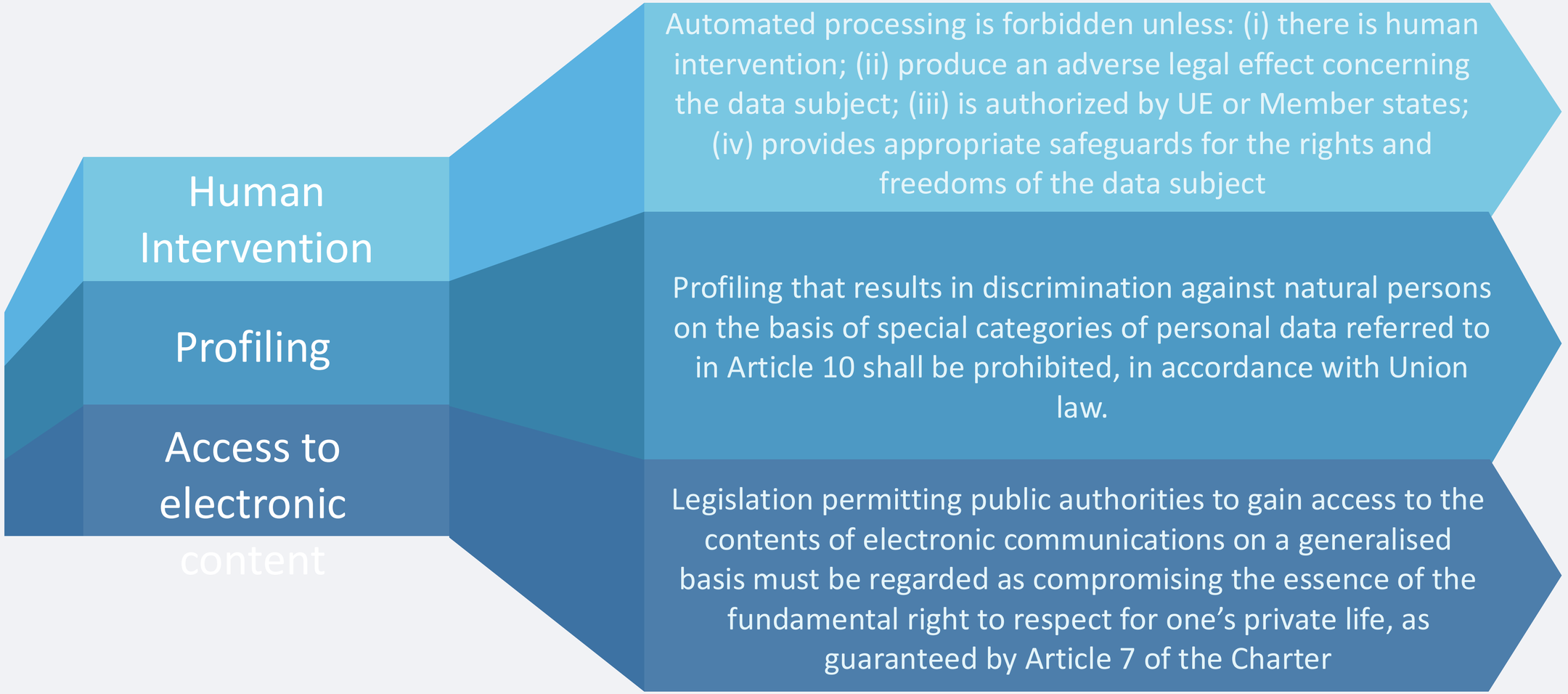
FACEFIRST

Keycrime 3
INTELLIGENCE SOLUTION

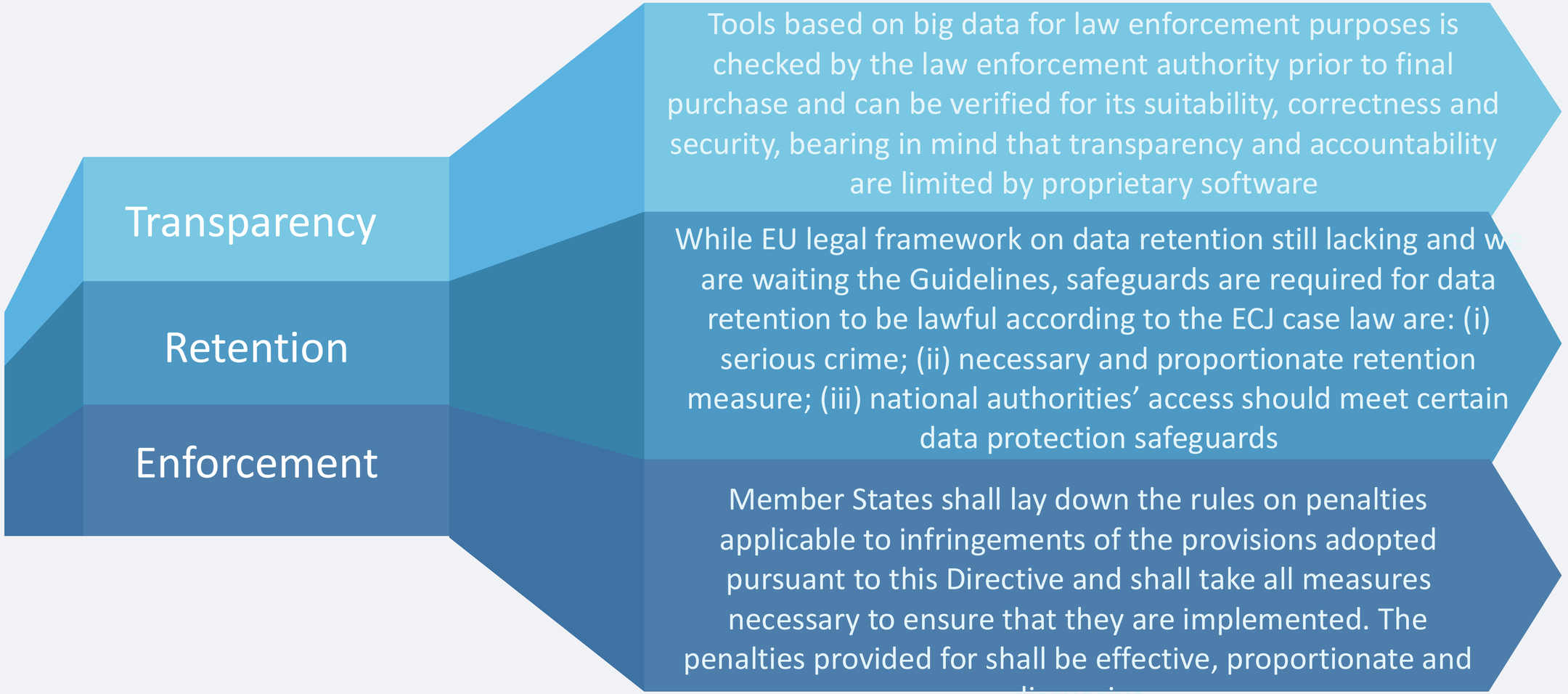
5 Pillars of “Police” Directive

- Fairly, lawful and adequate data processing during criminal investigations or to prevent a crime
- Clear distinction of the various categories of the possible data subjects in a criminal proceeding (investigated person, person convicted, victim of crime, third parties to the criminal offence)
- Prohibit measures which produce an adverse legal effect for the data subject or significantly affect, and which are based solely on automated processing of personal data
- Implementation of privacy by design and by default mechanism for ensuring the protection of the rights of the data subject and the processing of only those personal data
- Cooperation with the relevant supervisory authority by providing all information necessary to perform its duties

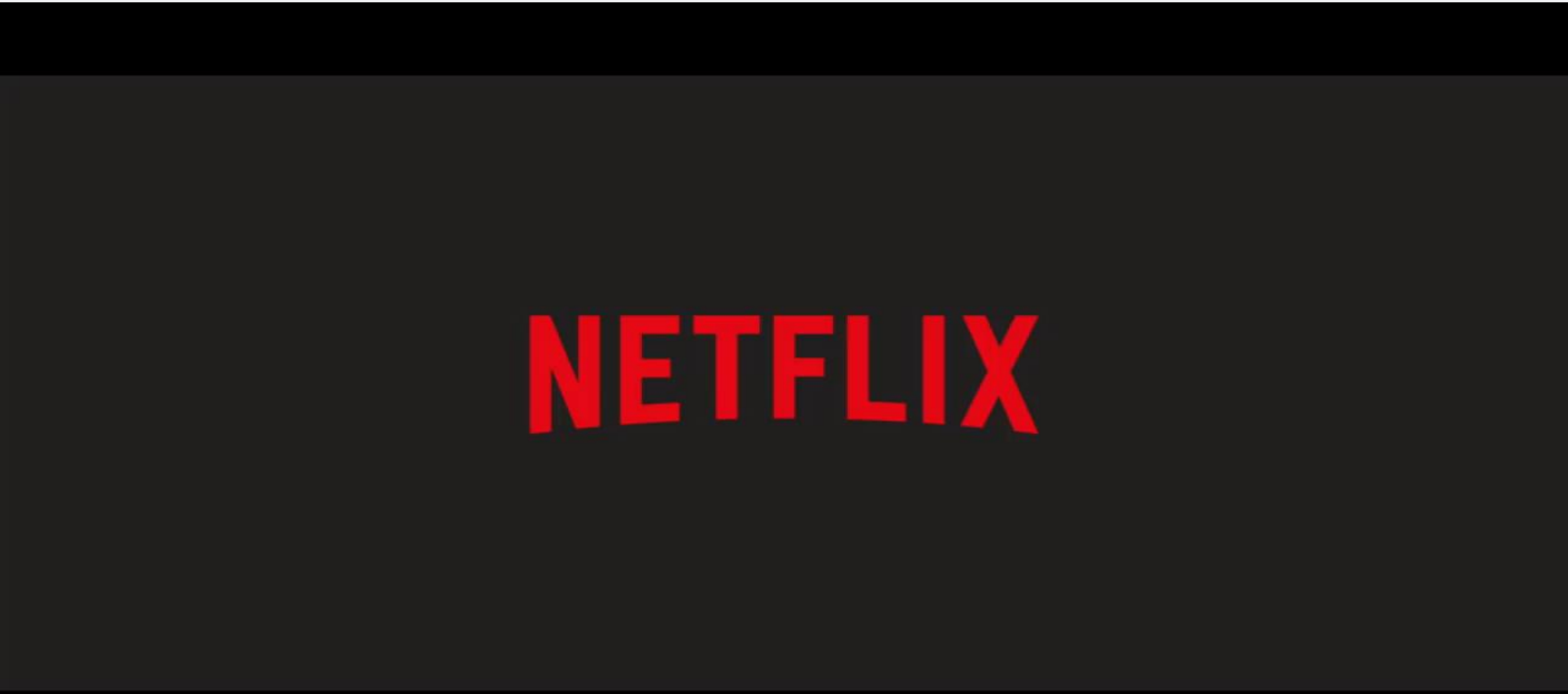
Automated Processing (art. 11 - ”Police Directive”)



Privacy vs Security: Again?



But what happens if security will win?



Budapest Convention on Cybercrime - Overview

🔎The Budapest Convention on Cybercrime was issued by the Council of Europe on November 23, 2001.

🔎Italy ratified the Convention with Law n. 48 on March 18, 2008, published in the Official Gazette on April 4, 2008.