Implementation of Article 15 of the Convention on Cybercrime in the Republic of Croatia

Prof. dr. Dražen Dragičević
University of Zagreb, Faculty of Law

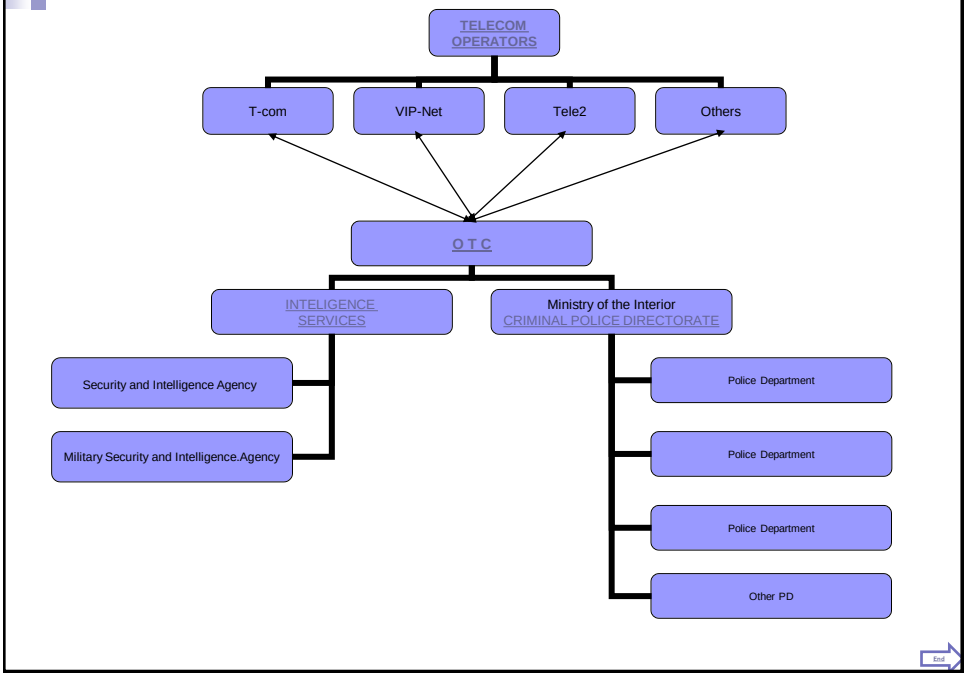
Introduction

Constitution of Republic Croatia

- High standards
  - Relevant international legal instruments for human rights protection are implemented in our legal order, most notably:
    - COE Convention for the Protection of Human Rights and Fundamental Freedoms
    - COE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, etc.
  - International treaties have primacy over domestic laws (art. 134)
    - „International treaties which have been concluded and ratified in accordance with the Constitution, published and which have entered into force are part of the domestic legal order of the Republic of Croatia and have primacy over domestic law.
- Principle of proportionality (art. 16)
  - Freedoms and rights may only be restricted **by law** in order to protect the freedoms and rights of others, the legal order, and public morals and health.
  - Any restriction of freedoms or rights must be **proportional to the nature of the need** to do so in each individual case.
- Section 3 of the Constitution („Protection of human rights and fundamental freedoms") guarantees, among others, right to **information** (art. 37) and **communication** (art. 36) **privacy**

Present situation

- Current state of croatian legislation is the result of:
  - Harmonization with EU law (*acquis communautaire)*
  - Implementation of CyberCrime Convention, additional Protocol and relevant COE recommendations (e.g. R(81)20, R(85)10, R(86)15, R(89)9, R(95)13 ..)
  - Bad experiences from the past



Implementation of procedural provisions of Cybercrime Convention with regard to conditions and safeguards

- With regard to measures implementing articles 16, 17, 18, 19 and 21 of the Convention relevant Croatian legislation provides, in total, adequate conditions and safeguards for the protection of human rights.
- With regard to the partial disclosure and real-time collection of traffic data there are some legal gaps and inconsistencies of rules which may benefit from legislative improvements. That especially refers to Police duties and powers Act.

Collection and disclosure of traffic data under the **Police Duties and Powers Act** (2009)

- **Police powers**
  - **.....**
  - **13. Verification of the establishment of telecommunications contacts**
- **Condition**
  - to prevent danger, violence, prevention and detection of criminal acts which are prosecuted officialy
- **Order**
  - written approval from the **head** of Criminal Police or a person authorized by him

- **Enforcement**
  - a police officer may require from the provider of telecommunications services verification of
    - **identity**,
    - **duration and frequency** of contact certain telecommunication address,
    - **identification of places** where are persons who establish telecommunications contact, as well as
    - **identification mark of the device**

Critics

- law does not require the existence of any minimum probability that the offense was committed or that the person has committed a criminal offense.
- applies to all police officers.
- not subject to any subsequent judical or any other effective external control.
- law does not prescribe who can be the person to whom the head of the criminal police of the Ministry may delegate his authority

Thank you for your attention!

"Control of information has been the essence of state power throughout history."
(Castells, M., Internet Galaxy)

Operator's obligations under the Electronic Communication Act (2008)

- **Secret surveillance of electronic communications networks and services** (Art. 108-110)
- Operators of public communications networks and publicly available electronic communications services must at their **own expense provide and maintain**
  - **the function of secret surveillance** of electronic communications networks and services, and
  - electronic communication lines to the **operational and technical body** responsible for surveillance of electronic communications.
- Operators are obliged to **retain the data on electronic communications**, in a safe manner and in its original form, for a period of **12 months**:
  - for the purposes of criminal investigations and prosecutions
  - for the purposes of national security and defense.

- Categories of traffic data to be preserve:
  - data necessary to trace and identify the **source** of a communication,
  - data necessary to identify the **destination** of a communication.
  - data necessary to identify the **date, time and duration** of a communication,
  - data necessary to identify the **type** of communication,
  - data necessary to identify users' communication **equipment** or what is considered as their equipment,
  - data necessary to identify the **location** of mobile communication equipment.
- **It is prohibited to retain data that reveal the content of communication.**

Operational Technical Centre for the surveillance of Telecommunications (OTC)

- Performs the measures of secret surveillance of telecommunication services, in accordance with:
  - SISA, for the purposes of national security and defense
  - CPA, for the purposes of criminal investigations and prosecutions
- O T C
  - performs the activation and manage measure of secret surveillance
  - realizes operational and technical coordination between:
    - the legal and physical persons that possess the public telecommunications network and provide public telecommunications services and access and
    - the bodies that are authorized to applicate the measure of secret surveillance of telecommunications in accordance with SISA and the CPA (SISA Art.18/1)
  - has the authority to oversight telecommunications service providers to fulfill that obligations.
  - has a direct access to the facilities and equipment of Ministry of Defence and armed forces and government bodies that have their own telecommunications networks.

Security intelligence system

- *Security Services Act* (2002)
  - Lack of coordination
  - Leak of information
  - Insufficient civilian oversight
  - Eavesdropping
- *Security Intelligence System Act* (2006)
  - **Parliamentary supervision** - is conducted directly or through the Parliamentary Committee for Domestic Policy and National Security
  - **Professional supervision** - is performed by the Office of the National Security Council
  - **Internal supervision** – is done by senior officials within the agency
  - **Civilian supervision** - is conducted by Council for Civilian Scrutiny of Security and Intelligence Agencies
  - **Judicial supervision -** measures of secret data collection may be undertaken only upon written reasoned order issued by a judge of the Supreme Court of the Republic of Croatia

Legal framework

- Police Act
- Criminal Procedure Act
- Police Duties and Powers Act
- Electronic Communications Act

Confidentiality request

- implemented in CPA (Article 231/1)
  - Procedure during the investigation is secret. The body that takes the action will warn the persons who participate in evidential action that the disclosure of secrets is a criminal offense.
- implemented in ECA (Article 15/7)
  - Persons who participate in the process of protecting computer data are required to keep as a secret information that they found out while performing their duties.