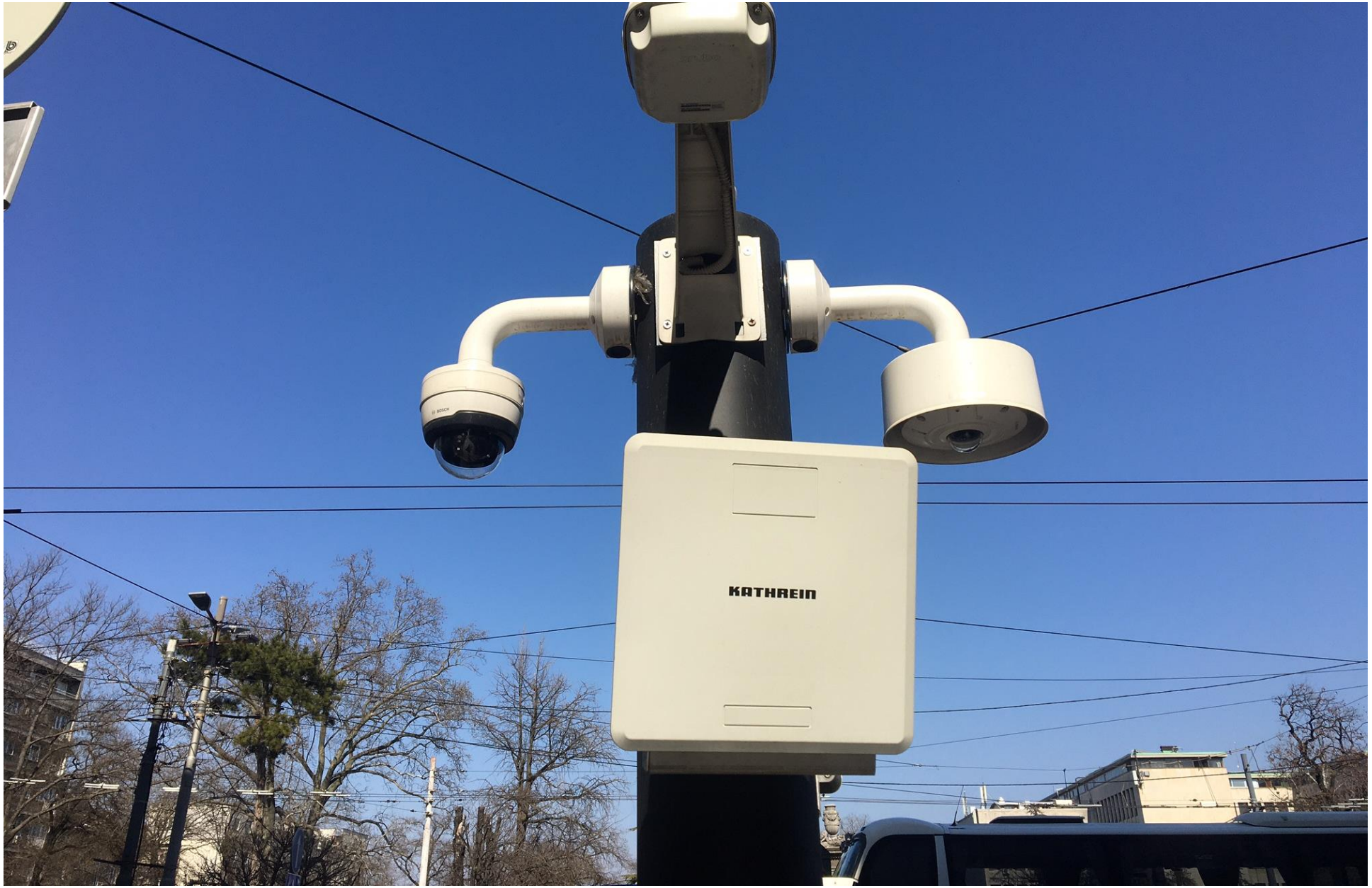
Smart city and surveillance technology in the light of Article 8 of the European Convention

dr hab. Marek Świerczyński, prof. ucz.

8 June 2022, Cracow



https://europeanwesternbalkans.com/2022/01/28/surveillance-technology-on-the-rise-in-serbia-a-threat-to-human-rights/

- Why the guidelines?
  - Governments resort to biometric techniques as the fight against crime depends to a great extent on the use of modern scientific techniques of identification.
  - Increased use of biometric techniques has significant impact on the people's fundamental rights.
  - Case-law of the European Court of Human Rights provide guidelines allowing to balance the potential benefits of the use of biometric techniques against important private-life interests

- Legal framework
  - Hard law
    - European Convention on Human Rights (Article 8)
    - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - Soft law
    - Guidelines on Facial Recognition
    - Guidelines on Artificial intelligence and Data Protection
  - EU legislation
    - General Data Protection Regulation
    - Law Enforcement Directive
    - Draft AI Act

- Fundamental principles
  - Use of biometric techniques by the public authorities should be legitimized under clear legislative framework.
  - The legitimate aim should be based on such values as national security, public safety or the economic wellbeing of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.
  - Legislation should ensure effective scrutiny over the applied measures based on biometric techniques.
  - Legislation should safeguard the data subjects' rights.

- Guidelines no. 1 - 3
  - Use of biometric techniques should balance the potential benefits of the extensive use of such techniques against important private-life interests.
  - The legislation should provide the necessary safeguards against abuse. Measures of this kind are to be ordered by the executive under control and with assessment as to whether they were strictly necessary. There should be an effective judicial or other remedy.
  - The amount of biometric data collected or recorded should be adequate, relevant, and not excessive in relation to the purposes for which they had been recorded.

- Guidelines no. 4 - 6
  - Biometric data should be retained for no longer than is necessary to fulfil the purpose for which it was recorded.
  - Use of biometric data should be limited to the purpose for which it was recorded.
  - Governments should provide guarantees aimed at regulating access to biometric data by third parties and protecting data integrity and confidentiality of such data.

- Checklist no. 1
  - Does the legislation pursue legitimate aim for applying such measures?
    - Can such interference with the right to privacy be classified as necessary in a democratic society? Is it supported by relevant and sufficient reasons and proportionate to the legitimate aim pursued?
    - Are the potential benefits of the use of such measures balanced against important private-life interests? Could the same objectives be produced using alternative, less harmful means?
    - Is the amount of biometric data to be processed adequate, relevant, and not excessive in relation to the purposes for which they had been recorded?

- Checklist no. 2
  - Does the legislation provide adequate and effective guarantees against arbitrariness and the risk of abuse?
    - Is the legislation sufficiently clear to give data subjects an adequate indication as to the circumstances in which, and the conditions upon which, public authorities are empowered to resort to any of such measures?
    - What specific safeguards are provided that are sufficiently precise, effective, and comprehensive in respect of the ordering and execution of such measures and for the securing of potential redress? Is there an effective procedure on review and supervision on the use of biometric techniques?
    - Does the legislation provide specific procedures on duration, storage, usage, access of third parties, the integrity and confidentiality of biometric data and its destruction? Is the data retained for no longer than is necessary to fulfil the purpose for which they were collected?

- Checklist no. 3
  - Are the data subjects' rights protected?
    - Do the data subjects have access to an effective and accessible procedures to allow them to have access to all relevant and appropriate information on the applied measures?
    - What effective judicial or other remedies are provided for the data subjects?
    - Is there a judicial procedure for the removal of biometric data from databases?

https://www.linkedin.com/in/marekswierczynski/

Marek Swierczynski

Attorney at Law IT/IP/Life Sciences

Warsaw, Mazowieckie, Poland · 500+ connections · Contact info

KRK Kieszkowska Rutkowska Kolasiński

Jagiellonian University