Issues in Cross-Border Police/Criminal Justice Data Flow in the European Union

Erich Schweighofer

http://www.univie.ac.at/RI/ES/
https://rechtsinformatik.univie.ac.at
https://deicl.univie.ac.at/

Arbeitsgruppe Rechtsinformatik
universität wien ARI
Centre for Computers and Law

universität wien

Outline

- Issues of cross-border exchange of digital police/criminal justice data
- International framework of data exchange between police/law enforcement agencies (LEAs)
- LEAs: data categories, databases & networks
- Exchange of evidence
  - International and European agreements, EU instruments
- Standards of digital evidence
- Respect for fundamental rights
- Data protection instruments
- Police and Criminal Justice Data Protection Directive
- Conclusions

Issues of cross-border exchange of digital police/criminal justice data (1)

- Admissibility: same legal guidelines as other forms of evidence but special rules and standards apply
- Particularities of digital data
  - Integrity and authenticity (original and not modified)
    - Electronic signatures and seals
    - Chain of custody (context of seizure highly relevant)
  - Procedural context of taking of evidence (what, where, when, why, and finally who)
  - Question of privacy
- Types
  - Databases
  - Digital documents
  - Digital traces
  - Communication/network data
  - Process data
  - Configuration data
  - Hardware data

Issues of cross-border exchange of digital police/criminal justice data (2)

- Forms
  - Fingerprints: ISO/IEC 19794 Information technology - Biometric data interchange formats
  - Evidence project
- Taking and recognition of evidence: territoriality + mutual recognition and assistance; *ordre public*
- Due process and respect for procedural rules
  - Data integrity – electronic evidence must not be modified in any way during the forensic process, including the initial data capture (except for technically justified reasons)
  - Chain of Custody = audit trail – a record of all actions must be taken when handling digital evidence must be created and preserved

Issues of cross-border exchange of digital police/criminal justice data (3)

- Type of procedure
  - Criminal procedure
  - Civil procedure
  - Police procedure
  - Administrative procedure
  - Intelligence data exchange
- Police procedure
  - Preventive investigation (prevention of danger)
  - Criminal investigation
- Criminal procedure
  - Criminal investigation

International framework of data exchange between police/law enforcement agencies (1)

- Question of trust
- Searches
  - INTERPOL
- Access to international/European databases by request
  - INTERPOL
  - Europol
- Direct access to international/European databases
  - Second Generation Schengen Information System
  - VIS, Eurodac
  - Convention of the Southeast European Law Enforcement Center (SELEC)
- Direct access to national databases
  - Treaty of Prüm
  - Hit/no-hit principle

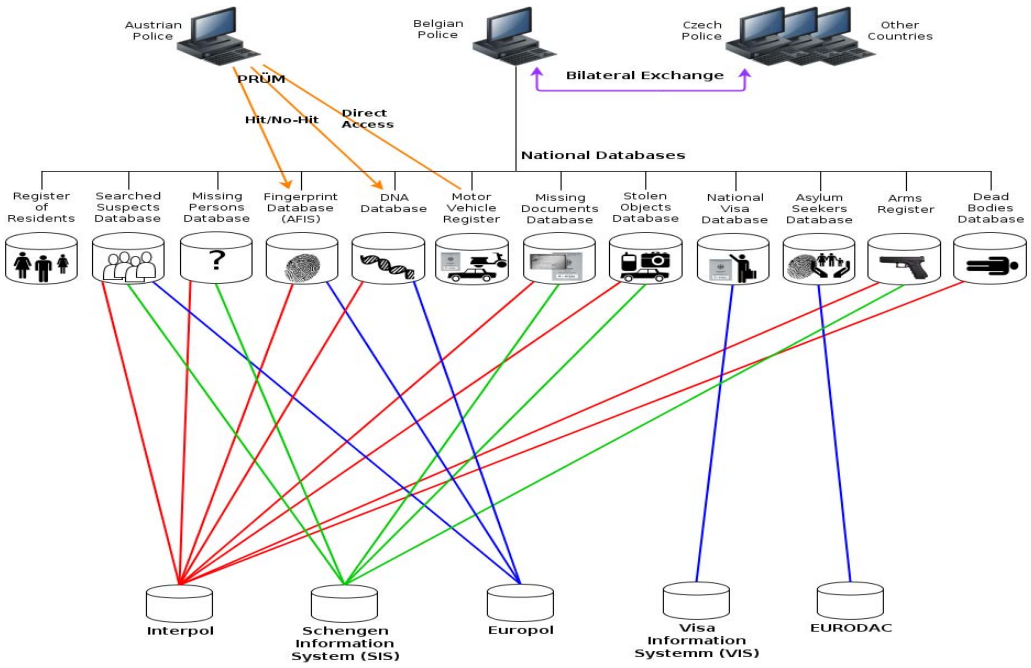
International framework of data exchange between police/law enforcement agencies (2)

- Access to national databases on request
  - Regional co-operation
    - PTN-collaboration of Nordic countries (P = politi (police); T = toll (customs) and N = nordisk (Nordic)
    - Police Cooperation Convention for Southeast Europe (PCC SEE)
    - Treaty between the Kingdom of the Netherlands, the Kingdom of Belgium and the Grand-Duchy of Luxemburg concerning trans-border police operations
  - Bilateral data exchange arrangements
    - Basic bilateral agreements (mainly concluded between a EU Member State and a third country)
    - Advanced bilateral agreements (mainly concluded between two EU Member States)
    - Bilateral agreements between neighbouring countries (some of which governing the establishment of a joint centre)
    - Bilateral agreements between an EU Member State and the United States of America (highly advanced and hence a distinct category)
      - "Prüm-like"

International framework of data exchange between police/law enforcement agencies (3)

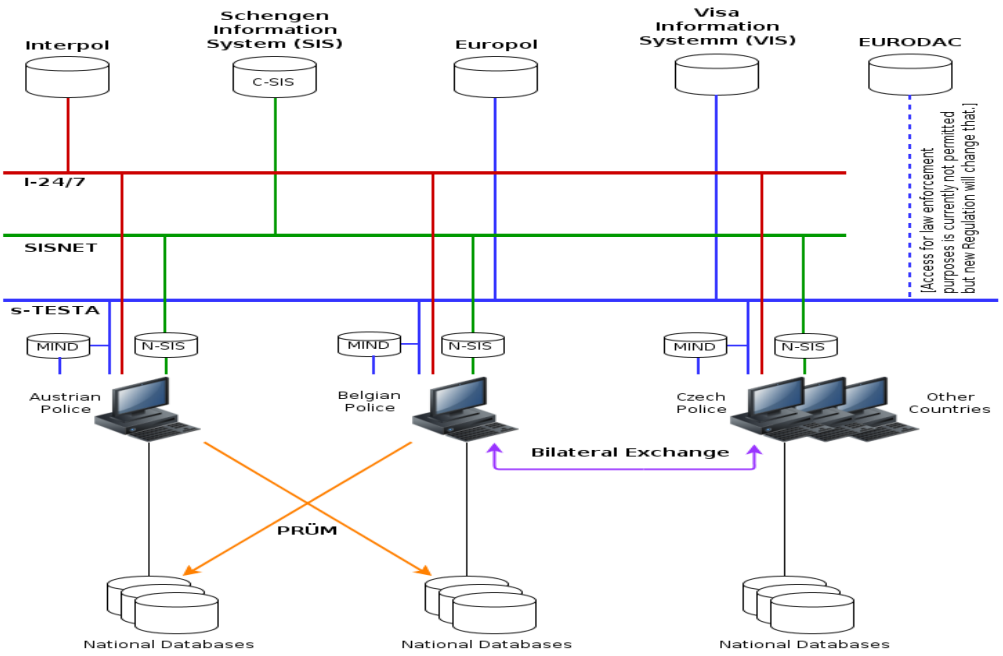
- Access to evidence
  - Bilateral co-operation
    - Advanced bilateral agreements EU-MS/EU-MS + bilateral agreements between neighbouring countries
  - European Investigation Order for criminal cases
  - Video
  - European Information Exchange Model (EIXM)
    - COM(2012) 735; Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement cooperation (2015)
    - Police Records Index System (EPRIS): no consensus
- Co-operation in affiliated areas
  - European arrest warrant
  - Freezing of assets and evidence
  - Confiscation orders
  - Exchange of information on convictions/criminal records
  - ECRIS (European Criminal Records Information Exchange System)

Law enforcement agencies: data categories & databases



universität wien

Law enforcement agencies: networks



universität wien

Exchange of evidence (1)

- Cybercrime Convention
  - Collecting electronic evidence subject to safeguards under national law (Art. 15)
  - Expedited preservation of stored computer data (Art. 16)
  - Expedited preservation and partial disclosure of traffic data (Art. 17)
  - Production order (Art. 18)
  - Search and seizure of stored computer data (Art. 19)
  - Real-time collection of traffic data (Art. 20)
  - Interception of content data (Art. 21)
  - 24/7 network (Art. 35)

- Other international law treaties (mostly superposed by Directive 2014/41/EU)
  - European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959 + additional protocols + bilateral agreements
  - Convention implementing the Schengen Agreement (CISA) + additional protocols
  - Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000 + protocol

Exchange of evidence (2)

- DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters
  - Transposition until 22 May 2017
  - Replaces/superposes EU 2000 Convention on mutual assistance in criminal matters, European Evidence Warrant Framework Decision 2008/978/JHA and Framework Decision on the execution of orders freezing property or evidence
  - Criminal cases, NOT preventive investigations
  - Judicial authorities (criminal, administrative or civil proceedings if the decision could give rise to proceedings before a criminal court)
  - Investigative measure
    - Necessary
    - Proportionate
    - Allowed in similar domestic cases
    - As soon as possible; 30 days for recognition and 30 days for execution
    - Same priority as in similar domestic cases

Exchange of evidence (3)

- Reasons for refusal
  - Immunity or privilege or rules limiting criminal liability relating to freedom of the press
  - Harm to essential national security interests
  - Non-criminal procedures
  - *ne bis in idem* principle
  - Extraterritoriality coupled with double criminality
  - Incompatibility with fundamental rights obligations
  - Lack of double criminality (except for a list of serious offences)
  - Impossible to execute the measure (investigative measure does not exist or is not available in similar domestic cases, and there is no alternative)

Exchange of evidence (4)

  - European Investigation Order
    - All investigative measures
    - Issuing authority – executing authority
    - Statements from suspects and witnesses
      - Onsite
      - Videoconferencing
    - Search and seizure to obtain evidence
    - Obtaining of information or evidence already in the possession of the executing authority
    - Interception of telecommunications (with additional safeguards)
    - Information on and monitoring of bank accounts
    - Excluded: Schengen cross-border surveillance by police officers and joint investigation teams
  - Mutual recognition but respect for fundamental rights (e.g. reason for refusal to execute)
  - Single standard form

Standards of digital evidence (1)

- Admissibility
  - Same legal guidelines as other forms of evidence but special rules and standards apply
    - eIDAS Regulation: e-signatures and e-seals
  - National rules on taking of evidence + mutual recognition
- Formats
  - Few rules (e.g. fingerprints); research projects (Evidence); practice
- Standards
  - CoE Guide on Digital Evidence
  - ACPO Good Practice Guide for Digital Evidence
  - Scientific Working Group on Digital Evidence (SWGDE)
  - ISO/IEC 27037:2012 Information technology -- Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

Standards of digital evidence (2)

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- OLAF: Guidelines on Digital Forensic Procedures for OLAF Staff (Regulation (EC) 883/2013, Regulation (EC) 2185/96)
- BSI: Guideline IT Forensics (Leitfaden „IT-Forensik“)
- ENISA: Identification and handling of electronic evidence & Forensic analysis - Local Incident Response
- CERT-EU: Incident Response – Data Acquisition Guidelines for Investigation Purposes
- CyberCrime@IPA: Electronic evidence guide - A basic guide for police officers, prosecutors and judges (restricted not for publication)
- ISACA (Information Systems Audit and Control Association): various, e.g. COBIT process (COBIT 5 framework for the governance and management of enterprise IT)

Standards of digital evidence (3)

- Practice or legally binding standards?
  - Practitioners: No standards but pragmatic practice (Hrdinka). Data are too complex and dynamic. Standards will lead to information loss.
  - Problem: training of police and courts is very challenging

Respect for fundamental rights (1)

- Right to privacy and/or information self-determination
  - Art. 8 para. 2 ECHR (protection of privacy and family life)
  - Art. 17 International Covenant on Civil and Political Rights (ICCPR) (protection of privacy and family life)
  - German informational self-determination right
  - German right to IT privacy
- Right to data protection
  - Art. 8 European Charta of Fundamental Rights
  - Art. 1 Austrian Data Protection Act

- Existing compliance mechanism, e.g. ECHR or Human Rights Committee

Respect for fundamental rights (2)

- Very relevant and interesting case law
  - Klass (1978, ECtHR)
  - Malone (1984, ECtHR)
  - Rotaru (2000, ECtHR)
  - Digital Rights Ireland, Seitlinger et al. (ECJ 2014)
  - Google Spain (ECJ 2014)
  - Max Schrems vs. Irish Data Commissioner (ECJ, preliminary ruling, ECJ 2015)
  - Szabó and Vissy vs. Hungary (ECtHR, 12 January 2016)
  - Tele2 Sverige AB gegen Post- och telestyrelsen und Secretary of State for the Home Department gegen Tom Watson u.a., (ECJ, C-205/15, 21 December 2016)
  - Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, (ECtHR, 27 June 2017)

Respect for fundamental rights (3)

- Informational self-determination
  - German Federal Constitutional Court, ruling relating to personal information collected during the 1983 census (BVerfGE 65, 1).
  - "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."
- IT privacy
  - German Federal Constitutional Court, ruling relating to on-line investigation, 27 February 2008, (1 BvR 370/07, 1 BvR 595/07)
  - Protection of data stored or processed in IT systems (part of personality right)

Data protection instruments (1)

- General Data Protection Regulation (GDPR)
  - Does not apply to:
    - Police/criminal justice
    - Intelligence agencies
    - Courts and other judicial authorities
      - Rec. 20 GDPR: Union or national law regulates the processing of personal data by courts and other judicial authorities
      - Art. 23 GDPR: “(f) the protection of judicial independence and judicial proceedings;”
      - Art. 23 GDPR: “(j) the enforcement of civil law claims.”
  - Exceptions for legal claims
    - Performance of a task carried out in the public interest or in the exercise of official authority (Art. 6 (1) (e) GDPR)
    - Sensitive data – Art. 9 GDPR: ”(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; “

Data protection instruments (2)

- DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
  - Most recent and detailed instrument at the moment
- Cybercrime Convention
  - No special rules, referring to national safeguards
- CoE Recommendation 87(15)
  - Visionary rules for data exchange between LEAs EUROPOL data protection rules
  - COUNCIL DECISION 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)
    - Purpose limitation, sensitive data, data security, access restrictions, safeguards

Data protection instruments (3)

- EUROJUST rules on data protection
  - College of EUROJUST 2005
- Proposed E-Privacy Regulation
    - COM(2017) 10 final
  - Applies not only to traditional telecoms operators, but also OTTs, e.g. new providers of electronic communications services, such as WhatsApp, Facebook Messenger, Skype, Gmail, etc.
  - GDPR modifications
  - Consent for communications data, both content and/or metadata gives traditional telecoms operators more business opportunities
  - New "cookie provision"; right to object to the reception of voice-to-voice marketing calls ("Robinson list"); more effective enforcement
  - No provisions concerning police/law enforcement

Police and Criminal Justice Data Protection Directive (1)

- Should be transposed into national law until 6 May 2018
- Follows strongly GDPR terminology and rules
- Applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art. 1)
- Court procedures: national rules, e.g. codes on criminal procedure apply
- Different categories of data subjects (Art. 6)
  - Suspects
  - Convicted
  - Victims
  - Other persons
- Distinction between personal data based on facts + personal data based on personal assessments (Art. 7)

Police and Criminal Justice Data Protection Directive (2)

- Lawfulness of processing (Art. 8)
  - Purpose is vaguely defined, subject to national laws on prevention of danger and criminal justice
    - Reuse not excluded, only more safeguards in certain cases
  - Necessary for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- Data subject rights (Art. 13 – 17)
  - Rights to information and access
  - Right to rectification or erasure of personal data and restriction of processing
  - Basic filter of not obstructing official or legal inquiries, investigations or procedures

Police and Criminal Justice Data Protection Directive (3)

- Data exchange to third countries or international organisations (Chapter V)
  - Purpose limitation principle
  - Law enforcement agency
  - Prior authorisation of Member State in case of further transfer of personal data
  - Adequacy decision or appropriate safeguards
  - Proportionality test for onward transfer
  - Appropriate safeguards (Art. 37)
    - Legally binding instrument
      - Existing international co-operation agreements: can be applied if they contain sufficient safeguards
      - Individual assessment of all relevant circumstances
  - Derogations for specific situations (Art. 38)
  - Transfers in individual and specific cases (Art. 39)

Conclusions

- Data exchange: trust is decisive
- Strong and complex international/European co-operation framework with data exchange
  - Access to databases, documents and digital traces
  - Police/law enforcement vs. courts
- Main instrument for data exchange between police/law enforcement: Directive 2016/680
- Purpose limitation principle
- Digital evidence
  - National laws with mutual recognition and international standards

universität wien

Thanks for your attention!

Erich Schweighofer

Universität Wien

Arbeitsgruppe Rechtsinformatik

Wiener Zentrum für Rechtsinformatik

erich.schweighofer@univie.ac.at
http://www.univie.ac.at/RI/ES/
https://rechtsinformatik.univie.ac.at

Jusletter IT
http://www.jusletter-it.eu

Central European Institute of Legal Informatics
http://CEILI.eu

universität wien

Questions are very welcome!

- LDA2017 Legal Data Analysis 2017 of CEILI at JURIX2017, 13-15 December 2017, 13 December 2017
- IRIS2018 International Legal Informatics Conference, 22-24 February 2018

universität wien