UNIVERSITÄT PASSAU
Juristische Fakultät

Evidentiary AI in Criminal Investigations – innovative approaches?

AI and the Protection of Privacy

Evidentiary Artificial Intelligence

- Judicial system designed around human interaction and testimony
- Potential use of evidentiary artificial intelligence
  - **Document review and analysis**
  - **Evaluation of existing witness evidence**
  - **Generation of new documentary evidence or witness testimony**
    - Interaction of AI and human
  - **Predictive analysis**
    - Use of data, statistical algorithms, and machine learning to identify patterns and make predictions about future events

Advantages from Using Evidentiary AI

- **Fast, efficient and comprehensive assessment** of substantial amounts of existing information
- Supply of **additional and new sources of information**
- **Consistency and standardization** in analysis of evidence and decision-making
- **Early detection** of emerging patterns or trends
- **Cost reductions** by automating labour-intensive tasks

Challenges with Evidentiary AI

- **Black box problem** = inability to adequately explain a certain outcome
  - **Lack of traceability** in the system's decision-making process and rationale
  - **Lack of transparency**
  - **Algorythmic bias**
- Reinforcing and reflecting existing **inequality and biases**
- **Misinterpretating or inadequate contextualizing information**
- Increasing **dependency on technology**
- **Dignity, (Data) Privacy** and **security risks**

Balancing AI and the Protection of Privacy

- **Human rights framework**
  - Right to Respect for Private Life, Art. 8 (1) ECHR
- **European Union framework**
  - Respect for the Private Life of Individuals, Art. 7 Charter of Fundamental Rights of the European Union
  - Protection of Personal Data, Art. 8 Charter of Fundamental Rights of the European Union
  - Directive 2016/680/EU [General Data Protection Regulation (GDPR)]
- **Constitutional framework**
  - General Right to Personality, Article 2(1) in conjunction with Article 1(1) of the Basic Law for the Federal Republic of Germany (German Constitution)

Right to Respect for Private Life, Art. 8 (1) ECHR

1. **Scope of protection**
   - **Private life** = sphere in which every person can freely develop his/her personality
   - **Protection of personal data**
     - Data = all information about a specific or identifiable natural person
2. **Interference**
     - Collection, storage and processing of data

Right to Respect for Private Life, Art. 8 (1) ECHR

3. Justification, Article 8 (2) ECHR

- Interference must be in accordance with the law
- **Clarity, foreseeability, and adequate accessibility of the law**
- Interference must be further a legitimate aim
- Measures must be **"necessary in a democratic society**"

Right to Respect for Private Life, Art. 8 (1) ECHR

- **Necessary in a democratic society**
  - **Reasons** adduced to justify the meaure must be **relevant and sufficient**
  - Interference must be **proportionate** to the legitimate aim pursued
  - **Balancing** the **public interest in the collection of data and the protection of private life**
    - Special requirements for sensitive categories of personal data (principle of lawfulness)
    - E.g. Personal data concerning criminal convictions and offenses, health data, biometric data, political opinions, religious or philosophical beliefs

Right to Respect for Private Life, Art. 8 (1) ECHR

ECtHR: „targeted interception“

1) [T]he **nature of offences** which may give rise to an interception order,
2) a **definition of the categories of people** liable to have their communications intercepted
3) a **limit on the duration** of interception
4) the **procedure** to be followed for **examining, using and storing the data** obtained
5) the **precautions** to be taken when **communicating the data to other parties**
6) the **circumstances** in which intercepted **data may or must be erased or destroyed**

Right to Respect for Private Life, Art. 8 (1) ECHR

ECtHR: „bulk interception“ (Big Brother Watch v. UK)

1) *the grounds on which bulk interception may be authorised;*
2) *the circumstances in which an individual's communications may be intercepted;*
3) *the procedure to be followed for granting authorisation;*
4) *the **procedures to be followed for selecting, examining and using intercept material**;*
5) *the precautions to be taken when communicating the material to other parties;*
6) *the **limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed**;*
7) *the procedures and modalities for supervision by an **independent authority** of compliance with the above safeguards and its powers to address non-compliance;*
8) *the procedures for **independent ex post facto review** of such compliance and the powers vested in the competent body in addressing instances of non-compliance.*

German Constitution: General Right to Personality

- Article 2(1) in conjunction with Article 1(1) of the Basic Law for the Federal Republic of Germany (German Constitution)

1. **Scope of protection**: Right to informational self-determination
2. **Interferences**: Collection, storage and use of data
3. **Justification**
   - Sufficiently specific legal basis („law“)
   - **Stringent proportionality test** using the **sphere theory**:
     - **Intimate sphere** = **core area of private life** – interferences not accessible to justification due to the dignity of the individual affected by them
     - **Private sphere** – interferences can be justified by overriding public interests
     - **Social sphere** – lowest intensity of interference

BVerfG, Judgment of 26 April 2022 – 1 BvR 1619/17 (Bavarian Protection of the Constitution Act)

(275) **intrusive surveillance measures**: **affected fundamental rights in conjunction with Art. 1(1) GG** give rise to additional requirements regarding the protection of the core of private life

(276) **core of private life:** the possibility of expressing internal processes such as emotions and feelings, as well as reflections, views and experiences of a highly personal nature // non-public communication with persons enjoying the highest level of personal trust, conducted with the reasonable expectation that no surveillance is taking place.

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Bavarian Protection of the Constitution Act)

(277) **surveillance measures**: protection of the core of private life be taking into account on **two different levels**

- **data collection stage:** safeguards to prevent the unintended collection of information relating to the core wherever possible
- **stage of subsequent data analysis and use:** consequences of an intrusion upon the core of private life that could not be prevented despite the presence of such safeguards must be strictly minimised

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Bavarian Protection of the Constitution Act)

(278)

- If the measure in question **typically leads to the collection of data** relating to the core, the **legislator** must enact **clear provisions** that ensure **effective protection**.
- Where the powers in question do not entail such a risk of core violations, it is not necessary to enact such provisions

  = **limits that directly arise from the Constitution** regarding access to highly personal information must be respected in the individual case
- **Surveillance of private homes**
- **Covert access to information technology systems**

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Surveillance of private homes)

(280) aa) Particular requirements apply at the **data collection stage**.

When assessing whether there is a probability that highly private situations will be recorded, **certain presumptions apply** in the interest of effectively protecting the core of private life.

Thus, **conversations taking place in private spaces with persons enjoying the highest level of personal trust** are presumed to belong to the core of private life and **may not be the target of surveillance**. The **automatic long-term surveillance** of spaces in which such conversations are to be expected is therefore **impermissible**.

This **presumption can be rebutted** when specific indications suggest that certain conversations are, within the meaning of the standards set out above, directly linked to criminal conduct.

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Surveillance of private homes)

(281) Thus, if a surveillance measure is likely to intrude upon the core of private life, the measure may **not be carried out**.

If, on the other hand, there are indications suggesting that certain conversations will not actually be highly confidential in nature, the measures may be carried out.

However, where the measures, despite no prior indications, result in the recording of highly confidential situations, **they must be discontinued immediately.**

If it is not clear whether a situation is highly confidential – for example due to language barriers – or if there are specific indications suggesting that, mixed in with highly private thoughts, criminal acts will also be discussed, surveillance in the form of automatic **recordings may be continued** (….).

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Surveillance of private homes)

(282) bb) Specific constitutional requirements also arise at the **stage of data analysis and use**. It must be ensured that the information obtained from the surveillance measure is **independently screened**. This also applies to the activities of the domestic intelligence services […].

The **independent screening process** serves both as a **review of lawfulness** as well as a **filter mechanism** to remove highly confidential data so that, **as far as possible, such data is not disclosed to the authority that carried out the surveillance**.

The body carrying out the independent screening must be provided with all the data originating from the surveillance of a private home (cf. ###).

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Surveillance of private homes)

(283) Although the case-law of the Federal Constitutional Court emphasises the necessity of having the **screening process carried out by an independent body**, this does not inherently exclude **the possibility of using an automated screening process**, provided that such a process is **technically feasible and reliable (or eventually becomes so at some point in the future)**.

The decisive point is that **no data** relating to the core of private life may **be disclosed to the authority that carried out the surveillance**, **beyond any information unavoidably revealed at the data collection stage** (…). The screening process, …, must not provide the authority that carried out the surveillance with an opportunity to derive (further) knowledge from the data.

BVerfG, 26 April 2022 – 1 BvR 1619/17 (Bavarian Protection of the Constitution Act)

Combined effect of surveillance measures

(287) Surveillance which takes place over an **extended period** and covers **almost every movement and expression** of the person under surveillance, and which could be used as the **basis for creating a personality profile**, is incompatible with **human dignity**.

BVerfG, 16 February 2023 – 1 BvR 1547/19 pp. (automated data analysis)

- Facts
  - Use of information technology in police work
    - § 25a HSOG (Hessian State Police Law)
    - § 49 HmbPolDVG (Hamburg Police Data Processing Law)
  - **Integrating automated files and existing data into analysis platforms**
  - Aim: Enhancing police work using advanced technology

BVerfG: Automated data analysis

- **Processing stored data sets using an automated application for data analysis or evaluation**
  - Interference with informational self-determination as an aspect of the General **Right to Personality, Article 2(1) in conjunction with Article 1(1) of the German Basic Law**
- **Weight of the interference** from automated data analysis or evaluation / requirements for its constitutional justification
  - Weight of **previous** data collection **interventions**: **Principles of purpose limitation and purpose modification**
  - Weight of **automated data analysis or evaluation itself**
  - Weight of the **interference** dependent on data type, extent, permitted analysis methods

BVerfG: Automated data analysis

- **Significant interference**
  - Justification only under strict requirements: Important legal interest (comparable to intrusive covert surveillance measures)
- **Enactment of regulations** on data type, extent and processing methods can be **divided between legislature and administration**
  - But legislative reservation needs to be preserved
  - **Legislature** must establish **fundamental principles** for limiting data type, extent, and processing methods
  - **Administration** is allowed to set **organizational and technical details**
  - Duty of legislature: Ensuring administration establishes documents, and publishes relevant guidelines and criteria for automated data analysis or evaluation in a standardized form

BVerfG: Automated data analysis

(77) In this respect, although the greater automation of police work does have the potential to prevent discrimination, it also harbours **specific risks of amplifying discrimination**.

These risks become less tolerable under constitutional law, the more the effects of automated data analysis/interpretation are capable of producing disadvantages that are prohibited under Art. 3(3) of the Basic Law.

BVerfG: Automated data analysis

(80) (b) The type and scope of usable data can also be limited by **statutory provisions** relating to the circumstances of the original data collection.

In particular, the **scope of the usable data** can be restricted by **purpose limitation rules** (see para. 55 ff. above).

If there are organisational or technical safeguards in place to ensure that data is only processed in accordance with its statutorily permitted use, and if the **statutorily permitted use** is defined in **sufficiently narrow terms**, the scope of data available for processing can be significantly reduced.

BVerfG: Automated data analysis

(86) (b) On the other hand, even though data analysis/interpretation makes use of vast quantities of data relating to a large number of persons, the overwhelming majority of whom have no involvement in the eventsin question, the severity of interference is reduced by the fact **that the data matching process is completed in a matter of seconds** and, in the **case of non-matches**, the collected data gives rise to **no further police action** (cf. …).

BVerfG: Automated data analysis

(89) (h) Technical and organisational safeguards can also be used to reduce the amount of personal data that is usable in data analysis/interpretation **by only granting access rights to a limited number of staff members who must satisfy particular criteria**.

If only a **small number of persons have access** to the analysis platform and access is only granted for precisely defined purposes, data analysis/interpretation measures are likely to be carried out less frequently and **less data will be processed**.

BVerfG: Automated data analysis

(90) The severity of interference is also influenced by the **permitted methods of data analysis/interpretation**. The use of complex forms of data matching can result in interference of a particularly serious nature.

If the police can make use of practically any existing IT method to extract far-reaching intelligence from the available data, **allowing them to identify new connections, generate new suspicions from multi-level analyses, and follow up by carrying out further steps in the analysis process or by instigating operational measures**, the impact of automated data analysis/interpretation on the persons concerned can be extremely adverse and the severity of the individual impairment can be significantly increased (cf. …).

BVerfG: Automated data analysis

(90) Furthermore, **with complex forms of data matching, the algorithms involved can be difficult to scrutinise**.

This has implications for individual legal protection and administrative oversight, both of which are rendered impossible without the ability to identify and rectify errors (cf. …).

In general, the severity of interference resulting from **the permitted methods of automated data analysis/interpretation depends on the breadth and depth of the personal information that can be generated, the extent of the margin of error, the likelihood of discrimination, and the difficulty of scrutinising the connections made by the software**.

Outlook

- Continued gradual adaption to technological advances
- National standardization, European and international harmonization
  - **Few existing legal frameworks**, standards on the balance between AI and the right to privacy [EU: AI-Act]
  - Framework continue to be set through **case law** Attempt to involve stakeholders with technological and legal expertise as early as possible
- Adversarial structure of the German criminal system
  - The individual himself must ensure himself that his rights are respected

Thank you for your attention!

Prof. Dr. Robert Esser

Universität Passau – Juristische Fakultät

Lehrstuhl für Deutsches, Europäisches und Internationales Strafrecht und Strafprozessrecht sowie Wirtschaftsstrafrecht

Forschungsstelle Human Rights in Criminal Proceedings (HRCP)

robert.esser@uni-passau.de