



EVEN

RECHTSANWÄLTE

Forensic Data Mining

A defence perspective

Agenda



1. Forensic Data Mining as a problem
2. Forensic Data Mining as a tool
3. A need for “transparency” in Forensic Data Mining

Forensic Data Mining as a problem

1.

Asymmetry of knowledge in investigations



- **Investigations often start as secret investigations**
- **Evidence is gathered through third parties** (e.g. search & seizure, wire tapping)
- **No right of the defence attorney to be present at the review of documents and no access to unreviewed documents and data pursuant to section 147** (BGH, judgment, 29.10.21, 5 StR 443/19).

Section 103 (1) s. 1 StPO:

Searches in respect of other persons are admissible only for the purpose of apprehending the accused or to follow up the traces of an offence or to seize certain objects and only if certain facts support the conclusion that the person, trace or object sought is located on the premises to be searched.

Section 110 (3) StPO:

The examination of electronic storage [...] on the premises of the person affected by the search is permitted. [...]. Data which may be of significance for the investigation may be secured.

Forensic Data Mining – a „black box“ in criminal investigations



The „organizational“ element

- Current practice (in white collar crime cases):
 - No or insufficient documentation of search strategy
 - no or insufficient documentation of search terms or of combination of search terms;
 - no or insufficient documentation of specific search results

The „outsourcing“ element

- Outsourcing of forensic data mining by Prosecutors (**Internal Investigations**):
 - Report of investigation process but not always detailed documentation of search process/terms;
 - Lack of access to “raw data” for individuals and their defence attorneys
 - Possible bias or limited scope of investigation depending on authority requesting the investigation (e.g. supervisory board, managing board)

The „technical“ element

- Assessment of review process is **complex** given the amount of different software used by prosecutors/police/internal investigations (e.g. X-Ways, NUIX, Relativity, etc.)
- Assessment of review process might entail additional costs for defence attorneys
- Assessment of review process will be “impossible” once **AI** is used to determine relevance of certain data/documents.

The „black box“ problem

Known Knowns

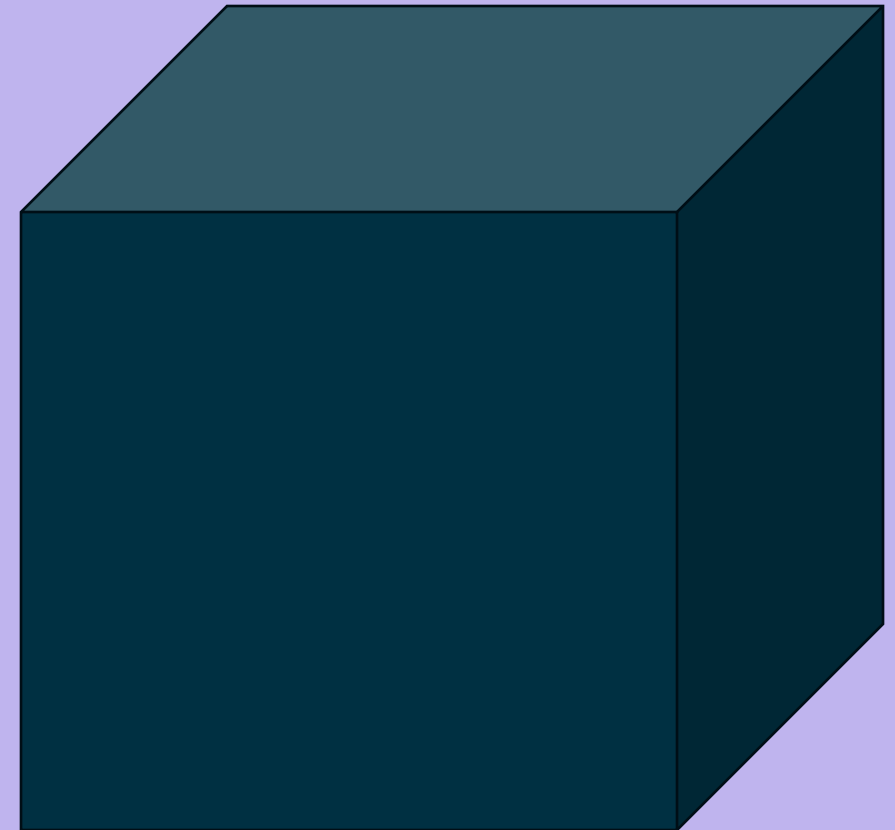
- Detailed information regarding search hits (documents considered relevant by Prosecutor/Internal Investigation)

Known Unknowns (Search Terms)

- Defence can assess what searches have **not** been made and what (potentially) exculpatory evidence has thereby **not** been found.
- “Raw data” remains a black box in bigger and complex cases

Unknown Unknowns (AI)

- Difficulty to assess what documents have **not** been consired by AI and for what reasons (case presented to AI as an indicator).
- “Raw data” remains largely a black box



Forensic Data Mining as a tool

2.

Forensic Data Mining as a tool



The best case scenario

- Client is willing and able to pay for Forensic Data Mining
 - Forensic Data Mining requires human involvement !
 - Software for Forensic Data Mining requires licencing
- „Raw Data“ is available
 - “Irrelevant“ data should be deleted (**What is „irrelevant“ data?**)
 - Prosecutor must be willing to share „raw data“

Problems for public defenders (Pflichtverteidigung)

- Lack of a clear ruling as to the circumstances under which the defence attorney can request that costs for licensing a forensic data mining software are reimbursed..
- The use of forensic data mining tools in the investigation phase (Ermittlungsverfahren) is practically impossible given the RVG-fee structure and extremely difficult during trial given the time constraints of trials.

See Graßie/Hiéramente in: Ory/Weth, jurisPK-ERV Band 4, 2. Aufl., § 147 StPO (Rn. 18)

A need for „transparency“ in Forensic Data Mining

3.

A need for transparency



Best Practices

- Public Prosecutor’s Offices and LKAs should prepare and publish „best practices“ regarding the use of Forensic Data Mining tools covering *inter alia*
 - A determination whether the software was used to review existing „evidence“ (Auswertung) or to determine whether data/documents ought to be considered as evidence (Durchsicht);
 - A determination whether the search is meant to retrieve all relevant documents (section 102-search) or only specific documents (section 103-search);
 - The documentation of the search strategy, specific search terms, specific searches;
 - The software used.

Reform of sections 102 et seq. StPO

- The legislator should prepare a comprehensive reform of sections 102 et seq. covering *inter alia*
 - A clear distinction between the review-phase (Durchsicht) and the assessment of evidence-phase (Auswertung);
 - A need for a prosecutorial decision that the review phase has been completed and the circumstances under which such a determination can be made;
 - a clarification that section 169a StPO requires a prior completion of the review phase.

Thank you for your
attention.

Impressum



EVEN Rechtsanwälte
Partnerschaftsgesellschaft mbB
Rothenbaumchaussee 5
20148 Hamburg

T +49 40 3611183-0
F +49 40 3611183-33
info@even.de
www.even.de