ORIGINAL RESEARCH

Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system

Monika Simmler[1] · Simone Brunner[1] · Giulia Canova[1] · Kuno Schedler[2]

Abstract

In the digital age, the use of advanced technology is becoming a new paradigm in police work, criminal justice, and the penal system. Algorithms promise to predict delinquent behaviour, identify potentially dangerous persons, and support crime investigation. Algorithm-based applications are often deployed in this context, laying the groundwork for a 'smart criminal justice'. In this qualitative study based on 32 interviews with criminal justice and police officials, we explore the reasons why and extent to which such a smart criminal justice system has already been established in Switzerland, and the benefits perceived by users. Drawing upon this research, we address the spread, application, technical background, institutional implementation, and psychological aspects of the use of algorithms in the criminal justice system. We find that the Swiss criminal justice system is already significantly shaped by algorithms, a change motivated by political expectations and demands for efficiency. Until now, algorithms have only been used at a low level of automation and technical complexity and the levels of benefit perceived vary. This study also identifies the need for critical evaluation and research-based optimization of the implementation of advanced technology. Societal implications, as well as the legal foundations of the use of algorithms, are often insufficiently taken into account. By discussing the main challenges to and issues with algorithm use in this field, this work lays the foundation for further research and debate regarding how to guarantee that 'smart' criminal justice is actually carried out smartly.

Keywords Smart criminal justice · Smart government · Algorithm · Artificial intelligence · Predictive policing

✉ Monika Simmler
  monika.simmler@unisg.ch

1   Competence Center for Criminal Law and Criminology, Law Schoool, University of St. Gallen, St. Gallen, Switzerland

2   Institute for Systemic Management and Public Governance, University of St. Gallen, St. Gallen, Switzerland

1 Introduction

Soon police officers may no longer be patrolling the streets, but robots could be strolling around cities checking parking spaces, issuing fines, and observing public spaces with potential for crime. The supervision and monitoring of crimes might be executed directly and in real-time from a central office which uses newest technical innovations to analyze, predict and solve crimes. Based on big data, surveillance technologies and automated decision-making, the system would automatically identify and prosecute offenders. We cannot foresee with any certainty whether or not the digital age is taking us there. However, it is a fact today that technical systems are increasingly playing an essential role in the work of police and criminal justice authorities, sometimes substantively changing their routines. In fact, a strong tendency towards the establishment of a 'smart criminal justice' (i.e., the use of intelligent technology in the criminal justice system) is currently observable (Simmler et al. 2021).

In particular, the phenomenon of predictive policing, along with other modern methods of crime prevention and prosecution such as data mining and face recognition technology, are rapidly gaining attention (Brayne 2021; Egbert and Leese 2021; Egbert and Krasmann 2020; Kotsoglou and Oswald 2020; Benbouzid 2019; Završnik 2019; Egbert 2018; Yu et al. 2011). Predictive policing tools promise to bring about a substantial revolution in policing and claim to be shaping the future of criminal justice. In response, the models underlying the algorithms, lack of empirical evaluation, potential racial disparity and reduction of a user's responsibility to defend their decisions have all been criticised (Bennett Moses and Chan 2018; Ugwudike 2020). Thus, it is evident that the criminal justice system is facing urgent challenges regarding its use of emerging technologies (cf. Završnik 2019). Nevertheless, research has yet to systematically deal with the implementation of advanced technology in the criminal justice system, in Switzerland and elsewhere. In contrast, studies have thoroughly addressed the fact that governments are discovering the use of advanced 'smart' technology to modernise the public sector (Gil-Garcia et al. 2016). In line with such general research on smart governance, it is necessary to devote scientific attention to the development of smart initiatives specifically in the criminal justice system.

In Switzerland, this debate is in its infancy (Cavelty and Hagmann 2021). Against this background and in anticipation of the further unfolding of the digital age, this study explores the reasons why and extent to which such a smart criminal justice system has been established in Switzerland, as well as the benefits currently perceived by users. In order to answer these questions, we conducted and systematically evaluated 25 qualitative interviews with 32 experts from 14 Swiss cantons. Based on these data, we argue that there is a need to thoroughly evaluate the effects of algorithm use in criminal justice, considering the legal foundations, as well as the accompanying psychological and institutional effects.

After a brief introduction to the phenomenon of smart criminal justice (Sect. 2) and presentation of the methodology (Sect. 3), this research presents the results of

the study (Sect. 4). Subsequently, the results are outlined and discussed, explicating the central challenges and guiding future research (Sect. 5).

2 Smart criminal justice

Smart government generally refers to the use of intelligent technology in the public sector, and thereby represents the further development of e-government (Gil-Garcia et al. 2016; Mellouli et al. 2014). Smart criminal justice, a sub-category of smart government, can be defined as *the use of technology in the criminal justice system based on algorithmic decision-making and the collection, analysis, and processing of big data* (Simmler et al. 2021). In the sense of this broad definition, criminal justice includes the work of the police, criminal judicial authorities, and penal system. In general, a smart criminal justice system seeks to leverage advanced technology and exploit its potential for more efficiency and effectiveness (Simmler et al. 2021).

As the definition indicates, not every use of a simple algorithm or process automation can be subsumed under the term 'smart criminal justice'. Broadly speaking, every digitization per se involves the use of algorithms, as basically any determination of 'if A, then B' qualifies as algorithmic. In the present study, the simple use of algorithms must therefore be distinguished from employment of advanced technology. However, the boundaries between e-justice (i.e., the simple digitization of processes) and smart justice are blurred (Lupo and Velicogna 2018). Therefore, a broad spectrum of applications is considered in a first step.

In order to categorise the various possible applications of advanced technology in crime prevention and law enforcement, we differentiate between the areas of *precrime* and *postcrime*. Due to different practical and legal implications, we further divide the area of *precrime* into (1) spatio-temporal predictive policing (i.e., the identification of possible crime scenes and times) and (2) predictive policing regarding individuals (i.e., the identification of potentially dangerous persons and subsequent threat management). In the area of *postcrime,* when a crime has already been committed, we distinguish between the use of (3) advanced technology in police investigations and (4) the subsequent criminal proceedings. Furthermore, we differentiate between the (5) forensic-psychiatric assessment of defendants during criminal proceedings and (6) the assessment of convicts in the penal system (see Fig. 1).

2.1 Spatio-temporal predictive policing

The term 'predictive policing' covers various methods for predicting crimes, based on probability calculations (Leese 2018; Uchida 2014). Such methods follow the assumption that crimes are subject to statistical regularities, and therefore statements about future crimes can be made based on past data. Predictive policing strives to identify possible crime scenes and times of occurrence. It relies on scientific findings such as the 'near repeat phenomenon' (Perry et al. 2013) and makes use of various forecasting techniques, including hot spot or risk terrain analysis, data mining, regression models, and spatio-temporal pattern recognition (Bennett Moses and

Chan 2018; Perry et al. 2013). The latest research has revealed the potential of such forecasting methods, but also emphasized the considerable costs associated (Rummens and Hardyns 2021).

2.2 Predictive policing regarding individuals

Predictive policing can also focus on the identification of potentially dangerous individuals (Berk 2021). In this domain, the police hope to prevent violent crimes through the early identification of threats and subsequent intervention and de-escalation (Simmler and Brunner 2021). Technology used in risk management is primarily intended to support the authorities in adequately assessing individuals and the risks they may present. In contrast to forensic-psychiatric assessments during ongoing criminal proceedings or in the penal system, these predictive policing measures are intended to take effect before a crime is committed. In this area, it was found that technical methods can substantially shape the way risks are assessed, producing new forms of algorithmic governance and of 'algorithmic risk' (Hannah-Moffat 2019).

2.3 Investigations and crime analysis

Deploying technology is no novelty in criminal investigations. Forensics relies heavily on filtering and evaluating relevant elements from large amounts of data (Burkhardt 2020). For instance, data mining methods are used to systematically analyse large datasets (Chen et al. 2004). Methods such as 'computer vision' (i.e., applications of visual recognition of objects, persons, and actions by means of machine learning) and speech recognition tools also support investigative work (Burkhardt 2020).

2.4 Criminal proceedings

Algorithms can be deployed to support legal assessments and decision-making in criminal proceedings. Although this field has not yet been developed to any great extent, various applications such as algorithm-based literature research and algorithmic evaluations of sentences are conceivable. In Estonia, for example, artificial intelligence (AI) capable of hearing and deciding small claims disputes is being developed and tested (Park 2020). Legal proceedings will most likely not remain unaffected by digital change (Brunner 2021; Villasenor and Foggo 2019).

2.5 Forensic-psychiatric assessment

Checklists and actuarial risk assessment instruments have long been standard in forensic psychiatry. They are based on the belief that in the field of short-term risk assessment, structured prognosis instruments are superior to expert opinions (Kilvinger et al. 2012). These instruments now serve as technical tools supporting assessments in ongoing criminal proceedings. In this category of smart criminal justice,

algorithms are mainly used to evaluate offender profiles and recidivism forecasts, eventually affecting sentencing.

2.6 Penal system

Algorithmic risk assessment instruments can not only be used in ongoing criminal proceedings for forensic-psychiatric assessment, but also in the penal system (e.g., to determine the need for further examination of a convicted offender or decide on execution mode, probation, and early release). As the algorithmic tools used in forensic-psychiatric assessments during criminal proceedings and in the penal system tend to overlap, these categories will be addressed together in this research (Fig. 1).

Users' perceptions of how these various algorithmic tools work and what they can do are a key factor in determining whether smart criminal justice will become widely adopted in practice. In a study on the 'uberization of policing', for example, Sandhu and Fussey (2021) found police officers to be skeptical about these tools if they did not trust the input data or could not understand how the algorithms worked. Conversely, Miro-Llinares (2020) argued that user acceptance of the new technology varied from optimism to pessimism, in a means analogous to most technology acceptance shifts in modern society. The present research examines the applications currently used in Swiss practice, why they were procured (i.e., the motivation), how they have been perceived by users, and what practical and scientific questions arise with respect to the future. In addressing these questions, this study provides a snapshot of the state of development regarding the use of algorithms in policework, criminal justice, and the penal system. Additionally, this study sheds light on the use of algorithms and accompanying opportunities and challenges, revealing avenues for further research not only in Switzerland but across the globe.
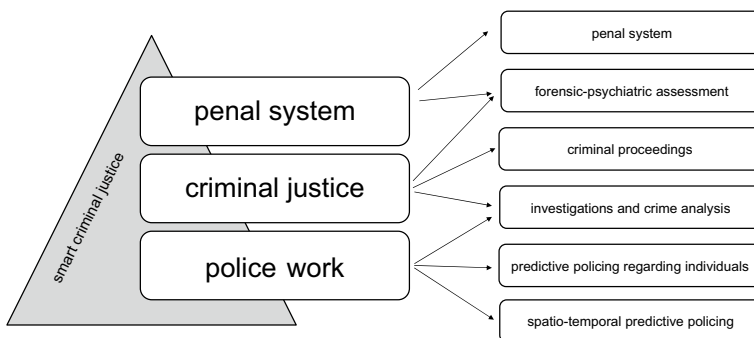

Fig. 1 Categories of smart criminal justice

3 Methodology

The findings presented below are the result of an empirical study conducted between April 2019 and February 2020, involving all cantons of Switzerland. The study followed an explorative approach to collect and structure data on a largely unknow research subject (cf. Becker 1993). Methodologically, the study used qualitative guideline interviews to build upon the knowledge and experience of experts directly confronted with the implementation and use of algorithms. The focus was not on the federal level, but rather on cantons (i.e., the 26 different states comprising the Swiss confederation, comparable to states in the US), as policing and criminal justice are mainly within their jurisdiction. To identify the relevant experts, we formed two groups consisting of either representatives of the cantonal police corps or of the penal system. To reach the relevant experts in these two groups, we contacted the cantonal justice and police departments. We then asked these departments to redirect us to experts using algorithmic tools. In doing so, we paid particular attention to including the widest possible range of expertise. At the same time, however, it was not possible to interview experts from all areas of interest in all cantons. In total, the study sample was composed of 25 interviews with 32 persons from 14 cantons. The interviews followed a uniform structure: the questions were defined in advance and were grouped according to the questions mentioned in the previous chapter. This led to a questionnaire including the following aspects: (1) demographic background of the participant, (2) algorithmic tools in use now as well as tools that may be used in the near future, (3) procurement process, (4) implementation and application of algorithms, (5) development and functioning of algorithms, (6) effects of the tools, (7) use of algorithms in risk assessment in particular, (8) legal foundations, (9) public communication of the use of algorithms and (10) avenues for further research.

By following a defined questionnaire, we aimed at achieving a sufficient level of comparability of the results. However, due to the explorative character of the research, the interviews did leave room for additional remarks from respondents. The sample ($N = 25$) consisted of 11 interviews with representatives of the penal system and 14 interviews with police officials. Of the total number of people interviewed (32), 11 worked in the penal system and 21 in the police corps; 26 (81%) were men and 6 (19%) were women. The role of the interviewees within their institutions varied. However, most of them (71%) were in a leading position (i.e. leading their specialised unit). Most of the interviewees were police officers (28%) or they completed a legal education (25%). Additionally, the group of interviewees was completed by psychologists (19%), criminalists (13%), computer scientists (6%), social workers (6%) or persons with pedagogical education (3%).

In order to capture (at least in outline) the use of algorithms in the 12 cantons where no representatives were personally interviewed, information was obtained by e-mail from 23 individuals. In total, 55 persons from 25 cantons were involved in the study. This overview of the algorithmic tools currently in use relied on this extended sample; the in-depth examination of the phenomenon, however, was based solely on the personal interviews, which were transcribed and qualitatively evaluated for this purpose.

The data analysis primarily consisted of a qualitative analysis of the semi-structured interviews. The qualitative analysis consisted of two steps that were executed for each aspect defined in the questionnaire: In a first round, we screened all interviews for the most important viewpoints and themes. Based on this, we developed an analysis raster and defined a numeric code. In a second round, we assigned the interview responses to the code in order to systematically obtain insights. The code comprised numbers for each question. We then analysed the interviewees' answers separately and assigned them to the number of the question they correspond to, regardless of whether the interviewees actually answered that exact question. This procedure allowed us to allocate the different pieces of information included in the answers to the right question as sometimes the answers did not match the question they followed but instead suit a different question contained in the questionnaire. Once we thematically sorted the answers, we conducted our analysis on two levels. On one level, we analysed the entire sample of respondents together and on a next level we analysed both groups of representants (police corps and penal system) separately. In addition, we evaluated whether there are striking similarities or differences between other groups of respondents (e.g., legal experts or non-experts). We then complemented the data with the information obtained from the e-mail survey which we previously analysed according to the same procedure as described above.

Although the interviews were carefully conducted to obtain additional information and cover as many algorithmic instruments as possible, it cannot be ruled out that the results are incomplete. It is possible that respondents did not have all the information at their disposal or other departments were using additional algorithms about which the respondents were not informed. There also might have been a range of understanding regarding what is considered an algorithm and should be named accordingly. As we contacted the interviewees via their departments, it cannot completely be ruled out that the departments provided respondents in manner that suited the respective attitude of the department regarding algorithmic tools best. In addition, it might be possible that confidentiality issues to some extend inhibited disclosure of information by interviewees. However, the interviewees were carefully selected and the results of the interviews were handled strictly confidential to minimize any influence of the departments distorting the results of the study.

4 Results

Our presentation of the results focuses on three central questions that turned out to be most essential: (1) what applications with which functionalities were available, (2) what the motives were for acquiring them, and (3) how they were being used and the benefits perceived by users (see overview in Table 1). Since motives for acquisition also reflect the expectations for the respective tools, they are related to the perceived benefits. Consequently, as a starting point, this study was concerned with the question of whether algorithms were deployed in the Swiss criminal justice system, and if so, at which institutions. The survey showed that all examined cantons used at least one algorithm-based tool, and many used several. However, most of these tools were not based on very advanced, complex, or self-learning technology. A

substantial percentage of the algorithmic tools resembled digital checklists or simple automation processes (i.e., 'e-justice'), and thus could not be classified as intelligent technology (i.e., 'smart justice'). Furthermore, this research discovered early on that in criminal courts and offices of public prosecutors, intelligent algorithms were thus far not in use. Hence, that area of inquiry received no further attention, though it certainly has the potential for future applications of smart criminal justice.

4.1 Applications, motives, and use

4.1.1 Spatio-temporal predictive policing

Currently, three Swiss cantons use an algorithm-based predictive policing tool that supports the prevention of burglaries and relies on self-learning techniques. The system named PRECOBS was developed and commercialised by a private institute based in Germany. The overarching goal of the tool in its standard version is to reduce the number of burglaries being committed. Based on recent crime data, it generates forecasts that allow the police to identify risk-prone areas at an early stage (cf. IfmPt 2018). The predictions rely on a 'near repeat' approach; after a burglary occurs, risk-exposed areas are identified (Schweer 2015). It is then assumed that based on past events or series of burglaries recorded in these areas, such areas could also be the target of future crime. Hence, the system makes use of geospatial modelling to generate risk profiles for locations (Shapiro 2017).

To generate predictions, PRECOBS requires a relatively small amount of data, consisting of information from police records of reported burglaries. Initially, the system extracts information regarding circumstances of a burglary including time, object, modus operandi, damage and exact geographical location. These parameters are then compared with reference catalogues of pre-identified trigger and anti-trigger criteria. Trigger criteria (e.g. a list of modi operandi) indicate future near repeats while anti-trigger criteria (e.g. the use of keys) oppose near repeats. Areas that are automatically identified as risk prone are then focused on in real-time police operations, e.g., by sending patrols (for more details see Gerstner 2018; Schweer 2015). Apart from the real-time analysis, PRECOBS verifies its predictions by retrospective simulation studies. Past predictions are evaluated by comparison with actual occurrences to confirm that the areas are suitable for accurate predictions (Gerstner 2018). Findings on successfully predicted near repeats are constantly reincorporated into the algorithmic tool (IfmPt 2018). This way, the data set is constantly being expanded based on past events which makes the tool a 'learning' system that features a certain level of intelligence. However, it is not based on machine learning in a narrower sense, as its predictions follow previously entered 'if–then' decisions.

4.1.1.1 Motives Regarding the acquisition of spatio-temporal predictive policing tools, the interviews revealed that the (dis-)proportion between costs and benefits was decisive. When reflecting on the benefits and effectiveness of such predictive policing systems, the respondents drew a variety of conclusions. Two of the three who used such a system were explicitly positive about its output and believed that it

helped achieve related policy goals. Conversely, the majority of the respondents who had chosen not to implement the program referred to the lack of evidence of its effectiveness and general uncertainty as to whether the benefits justified the cost. Other than this particular tool, no other algorithmic systems in the field of spatio-temporal analysis were deployed at the time of this study.

4.1.1.2 Use On an operational level, the tool mainly serves to reduce complexity by identifying patterns. Accordingly, the interviewees expressed that the system was only deployed to support the planning process; it did not give recommendations for action. The authority to decide what measures to take in a specific situation (e.g., whether or not to send additional patrols to critical areas) always remained with humans. Moreover, every result of the algorithm was subject to close scrutiny by the user. As it features algorithmic calculations, issues of transparency and comprehensibility seemed to accompany its use. Two out of three representatives from the cantons using this tool stated that its functioning was clearly understandable. The third representative described the underlying algorithm as not fully transparent.

4.1.2 Predictive policing regarding individuals

Predictive policing regarding individuals is especially important in threat management, which was institutionalised and professionalised in many Swiss police corps in the 2010s. The establishment of such specialised police departments was inspired by the conviction that risk indicators leading to violent crimes could be recognised early on, allowing for systematic risk assessments to identify threats and prevent escalation (cf. Brunner 2017). As the present study revealed, the majority of Swiss-German police corps currently use algorithm-based assessment instruments to support this process.

In contrast to other fields of smart criminal justice, no procedural standardization of predictive policing regarding individuals was observed. One of the tools used is a web-based application called 'Dynamic Risk Analyses System'. It is used to assess the likelihood of severe intimate partner violence. The static and dynamic items it incorporates correspond to specific questions related to potential risks of escalations in relationships. Each of the 39 items (i.e., questions) is assigned to a risk score ranging from 0 to 5 (cf. Hoffmann and Glaz-Ocik 2012). The overall risk calculation is based on a multi-layer set of rules with at least 50 interacting rules that yield a total risk score and four additional sub-results. The respondents, however, did not know anything about the detailed weighting or interacting of the items by the algorithm. The complexity of the underlying statistical calculations of this risk assessment process requires computational power beyond human capacities (Hoffmann and Glaz-Ocik 2012). However, the algorithmic system is not based on machine learning techniques but applies pre-defined rules (Sommerer 2020). As the survey showed, at least five cantons have already acquired this tool, though it has been partly abolished by some since the acquisition.

Another algorithm identified in the interviews was specifically tailored to the subject of radicalization. This tool conducts risk assessments using an online questionnaire. Although it was developed by a Swiss institute, the principles underlying

its development and technical details remain unknown. A more comprehensive risk assessment instrument was used by six cantons in the fields of extremism, domestic violence, and stalking. In this instrument, the dynamics of violence are determined according to eight dimensions, with each assessed according to a catalogue of different items. However, the tool does not produce any risk figure and is flexibly structured. Thus, it does not qualify as an algorithmic decision-making tool in any narrow sense. Although the survey showed a certain diversity in the tools used, it was clear that in most cantons, algorithms are already widely used in the process of identifying dangerous individuals.

4.1.2.1 Motives Regarding the motives for implementing algorithmic risk assessment instruments, respondents unanimously referenced political and media pressure in the aftermath of tragic crimes as a main reason for the expansion of preventive threat management, which in turn has led to further professionalization. As reasons against the acquisition of such algorithms, respondents mainly identified a lack of necessity due to low case numbers, as well as financial reasons. Some respondents also pointed out that no external evaluations of these tools were available, since the manufacturers monopolised their evaluation.

The advantages of using an algorithm serving as the motive for its implementation is a topic that deserves further consideration. The interviews revealed that actual benefits resulting from use played only a subordinate role. Respondents commonly stated that when it came to actually assessing a situation and deciding on what to do to prevent a crime, a single indicator such as the number or colour provided by an assessment tool was of rather low significance. Accordingly, respondents unanimously felt that the tool itself was not decisive, since such algorithms do not propose what measures to take to prevent crimes. Also, many interviewees emphasised that algorithmic checklists could not serve as a basis for decisions in this field, let alone an algorithm autonomously making such choices. In this regard, respondents further emphasised that human intuition and experience could not be replaced by algorithms. In sum, the majority of respondents confirmed that algorithms did not play a leading role in the overall assessment of critical cases. Nonetheless, they were relevant because they provide a clear structure for practitioners and thus guide the evaluative process to a certain degree.

4.1.2.2 Use According to those interviewed, algorithms were found to generate a considerable amount of added value. Such value primarily resided in the structured approach they provide, as the algorithmic process guides expert risk assessments and ensures that all relevant aspects are included. Second, added value was found in that such tools have led to a certain level of standardisation among experts through unification of terminology and procedures. Third, several respondents considered it particularly positive that individual assessments generated by these instruments always required justification, therefore encouraging users to reflect more deeply on their cases.

The question of whether the functioning mode of such algorithms was comprehensible to users was also of interest in this study. In this context, the survey detected a basic level of trust in the creators of these tools, as users tended not to question the way the algorithm and its variables were developed. None of the respondents expressed concern regarding the comprehensibility of such systems and the results produced. On the contrary, most respondents were convinced that the functioning was easily traceable. No one considered an in-depth understanding of the programming of an algorithm to be a necessary prerequisite for its use. However, this perception could also be related to the relative simplicity of the algorithms currently being employed.

4.1.3 Investigations and crime analysis

Crime analysis was another aspect of police work that was of interest in this study. Advanced technology in this field is designed to support the analysis of case-related data, profiling and identification of crime patterns. While such analyses usually involve various technical systems that are often developed in-house or based on generalist software such as Microsoft Excel, other specialised software is also deployed. Several police corps currently use a tool developed by the University of Lausanne to identify series of property crimes (PICAR). The tool does not make any calculations on its own, but rather allows for a structured collection of crime data such as the time, location, and modus operandi of the incident. As the analysis of connections between crimes is conducted by human analysts themselves, the underlying algorithms cannot said to be very advanced. It is rather a pure database allowing for further (potentially algorithmic) analysis.

In the field of cybercrime, a new tool is currently in use or being tested in certain cantons (PICSEL). This algorithm collects data in a systematic and structured way and identifies serial delinquencies in cybercrime. For example, indications of a possible series (e.g., by perpetrators repeatedly using the same e-mail address) can immediately be detected with the tool. Users are provided with an automated overview of possible links between offences. However, the tool does not classify as algorithmic decision-making or AI-application but rather constitutes a modern database allowing for identifying connections between cyberoffences.

In addition to the above-mentioned data structuring tools, all examined crime analysis units of the police departments explored for this research made use of additional data analysis tools. Such tools usually contained advanced technology for data analysis purposes. Two of the tools currently in use were developed by IBM. The survey showed that some police corps use the IBM i2 Analyst's Notebook and the IBM Watson Content Analyzer software to analyse large amounts of collected (digital) evidence. These programs assist digital forensics to systematically analyse unstructured data sets, especially seized evidence (SPIK 2016). IBM Watson is an AI-based application capable of discovering patterns in such large unstructured data sets (IBM 2019). It is powered by machine learning techniques and operates by deep

natural language processing (High 2012). Furthermore, IBM i2 Analyst's Notebook enables visual analysis to provide insights into complex data. Doing so, it relies on an Entity Link Property-model (Mak et al. 2018). The interviews further revealed that face recognition software was already being considered and evaluated, but was not in use at the time of the interviews.

4.1.3.1 Motives Criminal investigations have always essentially been based on data collection and analysis. Now, the digital age has made it possible to break new ground in this area. In this domain, the acquisition of technical tools is not really an innovation, and the motivation remains unchanged. Collected data must be analysed with as little effort and to as high a quality as possible. Technical progress allows practitioners to access ever-increasing amounts of data, a condition that in turn requires new data mining tools. As a further reason for the procurement of new instruments, the respondents noted that they can be used to optimize intercantonal cooperation and data exchange. For example, cybercrimes occurring in different cantons can be linked, and patterns in property crimes that transcend cantonal borders easily identified. However, according to the interviewees, there are still legal limits due to data protection requirements.

4.1.3.2 Use Regarding the benefits and effectiveness of such tools in the areas of investigation and crime analysis, the algorithms being applied were consistently positively appraised. These tools enable the networking of similar cases, and thus make identification of potential serial crimes much easier; as such, according to all respondents, they bring considerable added value in the sense of a qualitative improvement in police work. Likewise, none of the interviewees expressed any concerns regarding transparency, since no application involved complex calculations, and thus the tools in no way resembled a 'black box', lacking comprehensibility for forensic professionals.

4.1.4 Forensic-psychiatric assessment and the penal system

Forensic prognosis instruments are used in the penal system and criminal proceedings to assess the behaviour of defendants and risk of recidivism. As both fields utilize similar assessment instruments, they can be discussed together. The penal system is responsible for enforcing sanctions levied against convicted offenders. All cantons were found to use an algorithm embedded in a standardised concept of risk-oriented sanctioning. Although the system deployed in the German-speaking cantons differed slightly from the one currently being developed in the French- and Italian-speaking cantons, both systems appeared to be very similar and follow the same logic. The algorithm applied is a case screening tool for initial algorithmic case triage to determine if a person requires further clarification regarding correctional measures and enforcement decisions.

The system consists of weighted items, i.e. questions with a closed answer-format. The information for the answers is extracted from the offender's police file and criminal record. The tool categorizes cases as A, B, or C following predefined thresholds of values the algorithm calculates. Thus, this type of assessment-tool is based on simple linear models.

After the triage algorithm has determined the need for clarification, forensic prognosis instruments are usually consulted to support further evaluation. A variety of instruments are available, such as the 'Violence Risk Appraisal Guide' or classic 'Psychopathy Checklist'. These tools always function according to the same principle; they appear as checklists of varying levels of complexity, the result of which should contribute to a sound assessment of the dangerousness or risk of recidivism of a convicted person. They are algorithmic in the sense that they entail an 'if–then' decision structure. However, they deploy no intelligent or smart technology (yet), and the final judgment remains with the expert.

4.1.4.1 Motives In Switzerland, cantons' correctional departments enjoy a substantial degree of freedom in their concrete implementation of corresponding processes; thus, cross-cantonal coordination problems have repeatedly arisen. In response to a need for enhanced collaboration, a uniform enforcement concept was established in all German-speaking cantons in 2018, following the idea of a risk-oriented penal system. An analogue project has been initiated in the French- and Italian-speaking cantons. The interviews confirmed that the introduction of these systems was mainly justified by the desire for standardisation and increased efficiency in the penal system.

4.1.4.2 Use While the initial triage algorithm marks the beginning of every evaluation in the penal system, decisions regarding how and if further instruments will be integrated in the subsequent assessment process remain the purview of the evaluating expert. The same is true for evaluations of ongoing criminal cases, where the use of checklists is standard but not mandatory. As the interviews showed, no actual decision automation could be observed in the area of forensic assessment, at least after the triage algorithm identified the need for additional clarification. Rather, respondents stated that such tools tend to be used to structure and standardise the process. In addition, they allow for integration of the latest scientific findings and objectification of judgement. Even though the algorithmic output is considered, it is only one element among many other factors. It was often emphasised by interviewees that forensic assessments must always be conducted by a human. In contrast, only one respondent was of the opinion that human intervention could actually corrupt the results of forensic prognosis tools (Table 1).

Table 1 Synthesis: application, motives, and use

	Spatio-temporal predictive policing	Predictive policing regarding individuals	Investigation and crime analysis	Forensic-psychiatric assessment and penal system
Application	Scarcity: 3/26 cantons apply (self-learning) tools to prevent burglaries	Divergence: variety of tools widely applied to support risk assessment	Prevalence: analysis tools well established, increasing use of crime-specific data structuring tools	Harmony: standardisation by means of a single tool for all German-speaking cantons and another for all others
Motives	Expectation of preventive effects; cost-effectiveness as a crucial factor	Identifying dangerous individuals, thus allowing for preventive intervention; political and media pressure	Improvement in data analytics; efficiency gains; intercantonal cooperation and data exchange	Intercantonal harmonisation and standardisation; optimized use of resources
Use	Support for pattern identification and planning process; no automated decisions or actions; partly issues of transparency	Added value due to structured approach and standardisation; encourages further reflection on cases	No novelty, but improvement over previous work; linking of cases and series identification; calculations remain comprehensible	Initial triaging; supports, structures and standardises processes; integrates scientific knowledge; no automation

4.2 General findings regarding the use of algorithms

4.2.1 Driving forces and restraints

The above is an outline of the use of algorithms in different fields in the criminal justice system. Below, field-independent conclusions are described, based on the survey's findings; such conclusions allow for an overarching acknowledgment of the consequences of technology use and may pave the way for a smart criminal justice system.

Regarding the algorithms used, the question arises as to the motives underlying their acquisition and implementation. Considering the results of this study, various drivers and inhibitors of algorithm implementation can be identified. Political pressure, especially media pressure, was unanimously considered a driver of the (technically supported) expansion of predictive policing, as well as the intensification of risk orientation of the penal system. Accordingly, almost all respondents named key (criminal) events as decisive in the procurement of various tools. Furthermore, institutions that have developed instruments themselves promoted their establishment. Another driver, particularly in the penal system, was the need for efficiency and optimization of resources.

There are also many inhibitors to adoption, primarily consisting of a general scepticism regarding algorithmic systems and their effectiveness, as well as a rather negative, mistrustful attitude towards the automation of decisions. Some respondents stated that algorithmic tools could in no way replace human features, and abstract risk calculations could not fully guide the assessment of individual cases. The effectiveness of some applications was questioned, with reference to the data basis in Switzerland regularly being insufficient to carry out effective predictive analyses. A certain volume of data is needed for a (learning) algorithm to function at all, not to mention create added value. Most cantons are simply too small and do not have enough criminality to generate the amount and quality of data necessary. Likewise, threat management systems only work if the existing data allows for a well-founded use. Furthermore, financial considerations were identified as obstructing the implementation of certain tools.

4.2.2 Means rather than ends

Algorithms have become part of the daily routine of the criminal justice authorities. Therefore, this research further explored the perceived significance and embedding of algorithms in the respective institutions. Responses suggested that the tools had become part of the decision-making process, but mostly were not considered decisive components per se. Accordingly the respondents described them as guidelines, starting points, or common threads, but by no means autonomous decision-makers. For example, the use of risk assessment software allowed for a broad initial evaluation facilitating a grasp of the gravity of the case, and as such, presents just one out of many pieces to the puzzle. Algorithms were used to help structure the human assessment process, and especially to ensure that all relevant factors were taken into account. If the results of the algorithm indicated, for instance, a high degree of

danger or suggested possible burglaries at a location, interviewees stressed that this output had to be plausible to be used to justify further investigation. Furthermore, a tool might serve as a basis for (interdisciplinary) discussion within an institution or as a checklist to obtain relevant information from third parties. Respondents unanimously felt that no measures or interventions were based solely on the decisions of a tool.

The majority of respondents perceived the embedding of such technology in the decision-making processes as an opportunity to ask the right questions, rather than a tool for prescribing measures. The implementation of algorithmic tools was described as promoting general reflection on processes and often improving their structuring and standardisation, conditions welcomed by many respondents. Hence, algorithms were perceived as fostering standardisation and professionalization that could eventually lead to an increase in interoperability among the cantons (i.e., the promotion of better and more seamless cooperation). According to the interviewees, concepts such as standardised triage instruments in the penal system have led to the 'same language' being spoken, thus creating a common understanding of the cases being evaluated.

4.2.3 Human–machine interaction

Technology use is not only of overarching institutional relevance, but is also shaped by individual, psychological aspects of the human–machine interface. Among others, the decision regarding whether to purchase a tool at all was found largely to depend on the personal attitudes of decision-makers. This study found that interviewees who had decided to use algorithms tended to be convinced of their utility, while those who had decided otherwise were almost always critical. Interestingly, the scepticism expressed was mostly related to the effectiveness or concrete benefit of the tools, and not based on socio-political aspects or a fundamental rejection of the use of algorithms in the criminal justice system. Conversely, sceptical attitudes were opposed by proponents expressing the need for visionaries and pioneers (i.e., individuals with the courage to use the advantages of technology early on).

Once an algorithm was acquired, its practical application tended to be accompanied by various psychological mechanisms. Many respondents emphasised that they valued algorithmic tools because when they confirmed subjective findings, they lent confidence to the decision. Comparably, a 'gut feeling' was considered insufficient to justify measures or proposals to others and ensure external legitimacy, especially in the delicate field of criminal justice. If, for example, withdrawal of a firearms license was to be ordered, a subjective assessment of threat would not suffice. In such situations, algorithmic software could help to externally justify the assessment. Highlighting this approach was a statement from one respondent who believed that one could not 'simply listen to one's gut feeling'; otherwise, one would 'play the lottery'. At the same time, the perception of the algorithm as 'security' was contrasted with a paradox that manifested as follows. When interviewees were asked how they would act if the algorithm delivered a result other than their personal perception, almost all stated that they would trust their 'gut feeling'. The algorithm would not be blindly trusted but instead would be subject to verification and a plausibility check.

If a tool delivered a counterintuitive result, that result would be questioned and possibly overridden by the human. Conversely, if the algorithm confirmed the assessment of the user, it would serve as internal and external legitimation.

4.2.4 Effectiveness and evaluation

As indicated above, the effectiveness of algorithmic tools was appraised differently by the various respondents. Those critical of such tools argued that they often overestimated risk, and pointed to the lack of scientific evidence and absence of independent evaluations. Internal evaluations of their effectiveness have yet to be conducted by implementing authorities. On the contrary, respondents supporting the use of algorithms stated that the tools were a good way of incorporating the findings of current research into practice. Triage instruments and prognosis tools were described as containing empirically relevant factors necessary for proper assessment. Surprisingly, none of the interviewees criticized the fact that most instruments had only been evaluated by the developers themselves, and had yet to be subject to independent evaluation. Rather, it was affirmed that the impact of the preventive tools was difficult to evaluate because it was barely examinable whether the tools had actually contributed to crime prevention. However, all respondents expressed the desire to evaluate the effectiveness of the algorithms scientifically, if possible.

4.2.5 Accountability, law, and society

The socio-political discourse on the use of advanced technology in criminal justice is significantly influenced by the media. The majority of interviewees observed a 'media hype', which they perceived as 'exaggerated' and 'misplaced'. According to the respondents, the public and journalists often do not understand how algorithm-based tools actually work. In this regard, some respondents recognised that more proactive communication by officials could be helpful in generating public understanding and acceptance. Others, however, indicated that the general public isn't interested in the concrete ways such tools function. Media interest is only generated if offences occur. The public then demands prevention and a guarantee of security. As long as the use of algorithmic tools can be shown to meet these demands, they will be publicly supported.

Only a few respondents identified a need for legal changes due to the use of algorithms. It was occasionally mentioned that a lack of sufficient legal foundation results in uncertainties regarding the use of predictive policing regarding individuals. For this reason, some respondents expressed a desire for specific regulations regarding cases in which a crime has not yet occurred. However, most respondents were convinced that data protection was ensured, as the actions of criminal justice authorities are generally under the constant supervision of data protection authorities.

From the legal and societal perspectives, it was frequently brought up that accountability must be ensured when applying algorithms. The respondents considered accountability to be of special importance in the criminal justice system, especially for actions based on the algorithms' output. However, as the instruments now

in use are not very complex, the responsibility for decision-making currently fully remains with the human.

Accountability requires traceability and transparency regarding the algorithms in use. In this context, different attitudes among the interviewed could be identified. For most users, the algorithms' operation appeared accessible, even if individuals did not always understand the empirical basis and detailed algorithmic calculations. Occasionally, a desire for more background information was expressed. When it came to more complex algorithms, the respondents recognised the importance of traceability and transparency. In sum, the survey disclosed no in-depth examination of the legal and societal bases of technology use. This debate has not (yet) fully progressed in practice.

4.2.6 Possibilities and limitations of technology use

This study was not only dedicated to the analysis of the current state of affairs, but also interested in exploring how experts assessed future developments. The potential of algorithms was recognized particularly in terms of large computing capacities and the associated increase in efficiency, as well as qualitative improvement of analysis. However, most respondents made no concrete statements about the possible advantages of algorithms. Rather, there prevailed only a generic prognosis that algorithms could help to make more objective, better, and fairer decisions in the future. In sum, objectivity and transparency in decision-making were named as opportunities, and lack of the latter mentioned as a risk. Furthermore, a lack of trust in the algorithms could be perceived among a subset of the participants, and some even reported explicit mistrust of the developers.

A vast majority of the respondents perceived an expanded use of algorithms in the criminal justice system as unlikely, mainly due to the general public's prevailing fear of humans being replaced with algorithms. Among the experts, however, there was a broad consensus that algorithms could never fully replace human judgement, and that humans were and would remain superior to machines. Full automation of decision-making was rejected by all interviewees. In particular, the feeling was that algorithms would lack 'common sense', which is why, for instance, the possibility of replacing a human judge with an algorithm was considered unrealistic. Algorithms might make recommendations but could not take responsibility. Nevertheless, some of the interviewees stated optimistically that when it came to the future development and implementation of algorithms, the opportunities were far from exhausted and much potential remained untapped.

5 Discussion

5.1 A slow path towards smartness

This study revealed that various algorithms are in use in Switzerland. This trend, however, is unfolding slowly. Key criminal events and media pressure are crucial factors triggering the implementation of such algorithms. In this context, the use

of algorithmic tools is often an expression of a trend generally observable in Western legal orders: a shift from the repressive function of criminal justice towards an increasingly preventive policing approach (Carvalho 2016). This trend meets the increasing public desire for security and widespread zero tolerance of criminal threats.

Most of the algorithms used in the Swiss criminal justice system are relatively limited in their complexity, simply digitised versions of previously paper-based assessment instruments. With regard to the classification established here, this means that they constitute forms of e-justice. Most of the explored assessment instruments operated with a pre-defined set of rules or simple linear models. The main results of the study indicate that AI is only spreading marginally in Switzerland and currently only deployed in data analysis software. For now, data analytics remains the only application field for AI in the Swiss criminal justice system.

Thus, the prevailing level of automation and technical autonomy can be considered low (Simmler and Frischknecht 2020). The current state of affairs in Switzerland is not comparable to the situation in the US, where intelligent technology is rapidly expanding with the use of algorithmic risk assessment tools in criminal proceedings (PAI 2019), video surveillance based on automated facial recognition technology (Mann and Smith 2017), and other applications. This might be explained by the more limiting data protection and privacy laws in Western Europe.

Nevertheless, the implementation of algorithms at a low level of automation and complexity also leads to challenges and raises a multitude of questions. Since the criminal justice system can infringe on fundamental rights and freedoms, it must be ensured that its tools are subject to sound and continuous evaluation, and that the actors using such tools have sufficient technical know-how to apply them appropriately and justify the results.

Our study confirmed that the complexity of an algorithmic tool can become a problem for users if they are not able to understand the decision process (Miro-Llinares 2020). Conversely, algorithms can create transparency provided that they are comprehensible; this is in contrast to human decision-making, which largely remains inscrutable. Depending on the concrete field of application, it is important to determine the relevance of traceability, and thus the comprehensibility of decisions.

5.2 Techno-enthusiasts and techno-sceptics

The survey addressed respondents' respective mindsets regarding the implementation and effectiveness of algorithms used in the criminal justice system. Reviews varied; some respondents were sceptical, while others expressed positive, uncritical attitudes. This result is consistent with the finding that among attitudes regarding the deployment of intelligent technology, techno-enthusiasts are distinguishable from techno-sceptics (Guenduez et al. 2020). This inconsistency between different perceptions that was observed when researching public managers in general, may be especially relevant in the criminal justice system. The use of algorithms shapes (and will shape more intensely in the future) decision processes about crime threats, police reactions as well as even sanctioning and corrections. The quality of these

decision-making processes should not be based on individual differences of attitudes towards algorithms, but on scientific facts. Overly critical and uncritical attitudes can both be a hindrance to this.

Uncritical attitudes towards algorithms seemed connected with their role in the decision-making process. All respondents reaffirmed that the algorithms were by no means decisive components, and no measures or interventions were based solely on algorithmic decision-making. Algorithms were mostly perceived as guidelines, checklists, or starting points, as well as rather marginal factors in making decisions in the criminal justice system. These uncritical attitudes might at least partially be derived from the relative unimportance of algorithms in today's system.

Conversely, critical attitudes towards algorithms in general were derived from the fact that the connection between their use and decreasing crime rates is scientifically difficult to prove (Leese 2018; Gerstner 2017). There are only a few scientific evaluations of predictive policing instruments, and the methods upon which they are based are largely untested, let alone empirically evaluated by entities independent of the developer (Bennett Moses and Chan 2018; Uchida 2014; Perry et al. 2013). Furthermore, algorithms' effectiveness always depends on the quality of the processed data on the one hand, and training data on the other. However, data available to the police are inevitably incomplete and face various shortcomings (Leese 2018; Bennett Moses and Chan 2018). For example, the data underlying spatio-temporal predictive policing software do not always accurately represent the actual criminal activity in an area, as not all crimes are reported and registered (Bennett Moses and Chan 2018). These limitations should therefore be taken into account when evaluating such tools. In any case, evaluations should be conducted by independent authorities on a regular basis. Evaluations that are conducted by the developers themselves, especially if they are private companies, often contribute to further mistrust. Independent and more intense research is crucial to the further development of a smart criminal justice system, a fact not currently receiving sufficient attention.

5.3 Pseudo-legitimation?

This study highlighted the psychological components accompanying the use of algorithms in the criminal justice system. Individuals who had already acquired algorithmic tools generally expressed a positive attitude towards them, while those deciding against acquisition were sceptical. These results are consistent with general psychological findings (e.g., politicians tend to use information that supports their existing opinions and avoid using contradictory information) (Demaj 2015). A psychological explanation can also be found in so-called confirmation bias, which is the human tendency to interpret information to be consistent with one's own opinion (Nickerson 1998).

Not only can attitudes towards algorithms be affected by human psychology, but also their practical application. If the result of an algorithm confirms one's 'gut feeling' about an issue, it tends to be perceived as added security and a sign of external legitimacy. This perception of the algorithm as security is contrasted by a phenomenon we call the 'gut-feeling paradox': if the result of an algorithm is contrary to the

user's subjective perception, the feeling prevails and the counterintuitive algorithmic results are overridden. Therefore, the question arises as to whether an algorithm has any effect at all, or whether it merely operates as 'pseudo-legitimation'. Overriding the algorithm is simultaneously recognised as a great danger to the effectiveness of such tools, but also the only way to truly keep humans in charge. Up to a point, it must remain possible to doubt algorithmic output (Amoore 2019). However, how the gut feeling paradox actually unfolds in practice and the degree of automation most effective at facilitating an algorithm actually enhancing human decision-making should be the subject of further research. Users of algorithmic tools in criminal justice should be aware of the interdependencies that can arise between individual assessments and algorithm-based decision-making, and pursue a better understanding of these psychological effects (and ways to handle them).

5.4 Avoiding the 'black box' and legal uncertainties

In the past, algorithms have been accused of being a 'black box', lacking transparency or encouraging discrimination (Gabel Cino 2018; Završnik 2019); they should be subject to high legal standards, especially in areas where fundamental rights are at issue. Surprisingly, concerns regarding the ethics and lawfulness of the deployment of algorithms were scarcely expressed during data collection for this study. This might be due to the relative simplicity of the algorithms in use. Systematic biases and reinforcing feedback loops primarily affect self-learning and thus more autonomous algorithms, which are not yet widespread in Switzerland.

Furthermore, uncertainties about the legal foundation of predictive policing regarding individuals were disclosed. The fact that such uncertainties arise only after implementation of algorithmic tools is problematic (Simmler and Brunner 2021). In order to ensure lawfulness and prevent infringements on fundamental rights and freedoms, the implementing authorities must examine the legal foundation of the deployment of algorithm-based tools at an early stage. Such early-stage clarification of the legal foundations would also allow for transparent allocation of responsibility between algorithms and the humans who use them. This will ensure that the decision-making process is fully understood, guaranteeing not only legal compliance, but also general algorithmic accountability (Binns 2018).

5.5 Future perspectives

It is probable that the use of algorithms will further intensify in various areas and Switzerland will move towards a smart(er) criminal justice. Yet, complete automation of more complex processes in the administration of criminal justice is clearly problematic, as this study has shown. A general scepticism about the increasing use of algorithms was found, which is widespread among the public (Schedler et al. 2019). The attitude that responsibility resides and should remain with the individual is predominant. Enhanced public acceptance of the use of algorithms could be achieved by early and more active involvement and an intentionally open discussion. However, a scientific or political discussion about the implementation of algorithms

in criminal justice has yet to be held. Such an open discourse is by all means crucial to their legitimation and widespread acceptance of their use. Policymakers must actively promote such a debate regarding the potential and limitations of algorithm use in the criminal justice system. It was confirmed, however, that advanced technologies are reframing criminal justice debates in many ways (cf. Hannah-Moffat 2019).

6 Conclusion

Advanced technology is capturing the attention of criminal justice practitioners around the globe. Algorithm-based tools are designed to predict where and when future crime will happen, identify potentially dangerous persons, and calculate recidivism rates. This development is reflected by a strong tendency to encourage the establishment of a smart criminal justice. Drawing on a qualitative study, this research provides an overview of the algorithms used in the Swiss criminal justice system. We discovered that algorithm-based tools are mainly used in predictive policing, crime analysis, and forensic-psychiatric assessment. Generally, the level of complexity and autonomy of these algorithms remains low; they are rarely based on advanced self-learning, and therefore 'smart' technology. Nevertheless, algorithms are gaining importance in criminal justice because they are part of the decision-making processes, even though they mainly serve as support for the humans in charge. As soon as algorithms are deployed and in any form become part of the criminal justice system, questions related to their implementation, effectiveness, legal foundation, and accountability arise. We argue that practice and research must face the challenging questions regarding what standards algorithm-based technology must meet and what an adequate and effective use of algorithms looks like. In so doing, institutional and psychological phenomena emerging with the use of advanced technology must be taken into account. Above all, an actual societal and legal debate on the opportunities and risks must be held. In the digital age, this debate should focus on optimally shaping the interaction of human and machine and enhancing their respective strengths. To this end, neither fundamental criticism of algorithms nor blind and unreflective trust in their developers is useful. In conclusion, this study has shown that the emerging 'smart criminal justice' is promising, but factual, legal, and political limits will determine the boundaries of this development.

Declarations

References

Amoore L (2019) Doubt and the algorithm: on the partial accounts of machine learning. Theory Cult Soc 36(6):147–169

Becker FG (1993) Explorative Forschung mittels Bezugsrahmen: ein Beitrag zur Methodologie des Entdeckungszusammenhangs. J Res Hum Resour Manag 11:111–127

Benbouzid B (2019) To predict and to manage: predictive policing in the United States. Big Data Soc 6(1):1–13. https://doi.org/10.1177/2053951719861703

Bennett Moses L, Chan J (2018) Algorithmic prediction in policing: assumptions, evaluation, and accountability. Polic Soc 28(7):806–822. https://doi.org/10.1080/10439463.2016.1253695

Berk RA (2021) Artificial intelligence, predictive policing, and risk assessment for law enforcement. Ann Rev Criminol 4(1):209–237. https://doi.org/10.1146/annurev-criminol-051520-012342

Binns R (2018) Algorithmic accountability and public reason. Philosophy Technol 31:543–556. https://doi.org/10.1007/s13347-017-0263-5

Brayne S (2021) Predict and surveil: data, discretion, and the future of policing. University Press. https://doi.org/10.1093/oso/9780190684099.001.0001

Brunner R (2017) Herausforderungen in der praktischen Umsetzung des Bedrohungsmanagements, Erfahrungen der Kantonspolizei Zürich. Format Mag 7:4–9

Brunner S (2021) Automatisierung der rechtsprechung eine rechtstheoretische analyse. In: Simmler M (ed) Smart criminal justice. Helbing, Basel, pp 213–236

Burkhardt L (2020) Künstliche Intelligenz in der Strafverfolgung. Kriminalistik 5:336–345

Carvalho H (2016) The preventive turn in criminal law. University Press, Oxford

Cavelty MD, Hagmann J (2021) The politics of security and technology in Switzerland. Swiss Political Sci Rev 27(1):128–138. https://doi.org/10.1111/spsr.12430

Chen H et al (2004) Crime data mining: a general framework and some examples. Computer 37(4):50–56. https://doi.org/10.1109/MC.2004.1297301

Demaj L (2015) Information for politics: the polarizing effect of performance budgets on legislators' allocation judgments. Dissertation, University of St. Gallen

Egbert S (2018) About discursive storylines and techno-fixes: the political framing of the implementation of predictive policing in Germany. Eur J Secur Res 3:95–114. https://doi.org/10.1007/s41125-017-0027-3

Egbert S, Krasmann S (2020) Predictive Policing: not yet, but soon preemptive? Polic Soc 30(8):905–919. https://doi.org/10.1080/10439463.2019.1611821

Egbert S, Leese M (2021) Criminal futures, predictive policing and everyday police work. Routledge, London

Gabel Cino J (2018) Deploying the secret police: the use of algorithms in the criminal justice system. Georgia State Univ Law Rev 34(4):1073–1102

Gerstner D (2018) Using predictive policing to prevent residential burglary: findings from the pilot project p4 in baden-Württemberg, Germany. Eur Law Enforc Bull 4:113–123

Gerstner D (2017) Predictive Policing als Instrument zur Prävention von Wohnungseinbruchsdiebstahl. Max Planck Institute for the Study of Crime, Security and Law, Freiburg im Breisgau

Gil-Garcia R, Zhang J, Puron-Cid G (2016) Conceptualizing smartness in government. Gov Inf Q 33(3):523–534

Guenduez AA, Mettler T, Schedler K (2020) Technological frames in public administration: what do public managers think of big data? Gov Inf Q 37(1):1–12

Hannah-Moffat K (2019) Algorithmic risk governance: big data analytics, race and information activism in criminal justice debates. Theor Criminol 23(4):453–470

High R (2012) The era of cognitive systems: An inside look at IBM Watson and how it works. IBM, Armonk.

Hoffmann J, Glaz-Ocik J (2012) DyRiAS-Intimpartner: Konstruktion eines online gestützten Analyse Instruments zur Risikoeinschätzung von tödlicher Gewalt gegen aktuelle oder frühere Intimpartnerinnen. Polizei & Wissenschaft 2:45–57

IBM (2019) IBM Watson enables your business to get started with text-analytics. https://www.ibm.com/blogs/watson/2019/12/ibm-watson-enables-your-business-to-get-started-with-text-analytics/. Accessed 1 February 2022

IfmPt (2018) Predictive policing made in Germany. http://ifmpt.de. Accessed 10 February 2021

Kilvinger A et al (2012) Risikokalkulation bei häuslicher Gewalt. Fortschritte der Neurologie Psychiatrie 80(6):312–319. https://doi.org/10.1055/s-0031-1273200

Kotsoglou KN, Oswald M (2020) The long arm of the algorithm? Automated facial recognition as evidence and trigger for police intervention. For Sci Int Synergy 2:86–89. https://doi.org/10.1016/J.FSISYN.2020.01.002

Leese M (2018) Predictive policing in der Schweiz: Chancen, Herausforderungen, Risiken. In: Zogg B et al (eds) Bulletin 2018 zur schweizerischen Sicherheitspolitik. ETH Zurich, Zurich, pp 57–72

Lupo G, Velicogna M (2018) Making EU justice smart? Looking into the implementation of new technologies to improve the efficiency of cross border justice services delivery. In: Rodríguez Bolívar M (ed) Smart technologies for smart governments. Springer, Cham, pp 95–121

Mak K et al (2018) Wissensentwicklung mit IBM Watson in der Zentraldokumentation (ZentDok) der Landesverteidigungsakademie. Bundesministerium für Landesverteidigung, Wien

Mann M, Smith M (2017) Automated facial recognition technology. Univ South Wales Law J 40(1):121–145

Mellouli S, Luna-Reyes L, Zhang J (2014) Smart government, citizen participation and open data. Inform Polity 19(1):1–4

Miro-Llinares F (2020) Predictive policing: utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement. Idp-Internet Law Polit 30:1–18. https://doi.org/10.7238/idp.v0i30.3223

Nickerson RS (1998) confirmation bias: a ubiquitous phenomenon in many guises. Rev Gen Psychol 2(2):175–220. https://doi.org/10.1037/1089-2680.2.2.175

Park J (2020) Your Honor, AI. https://hir.harvard.edu/your-honor-ai/. Accessed 7 April 2021

Partnership on AI (PAI) (2019) Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System. https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/. Accessed 12 February 2021

Perry WL et al (2013) Predictive policing: the role of crime forecasting in law enforcement operations. RAND Corporation, Santa Monica

Rummens A, Hardyns W (2021) The effect of spatiotemporal resolution on predictive policing model performance. Int J Forecast 37(1):125–133. https://doi.org/10.1016/j.ijforecast.2020.03.006

Sandhu A, Fussey P (2021) The "uberization of policing"? How police negotiate and operationalise predictive policing technology. Polic Soc 31(1):66–81. https://doi.org/10.1080/10439463.2020.1803315

Schedler K, Guenduez AA, Frischknecht R (2019) How smart can government be? Exploring barriers to the adoption of smart government. Inform Polity 24(1):3–20. https://doi.org/10.3233/IP-180095

Schweer T (2015) «Vor dem Täter am Tatort» – musterbasierte tatortvorhersagen am beispiel des wohnungseinbruchs. Die Kriminalpolizei 1:13–16

Shapiro A (2017) Reform predictive policing. Nature 541:458–460. https://doi.org/10.1038/541458a

Simmler M, Brunner S (2021) Das Kantonale bedrohungsmanagement: rechtliche grundlagen eines neuen polizeiparadigmas. In: Simmler M (ed) Smart criminal justice. Helbing, Basel, pp 165–188

Simmler M, Frischknecht R (2020) A taxonomy of human-machine collaboration: capturing automation and technical autonomy. AI Soc. https://doi.org/10.1007/s00146-020-01004-z

Simmler M, Canova G, Schedler K (2021) Smart criminal justice: phenomena and normative requirements. Int Rev Admin Sci. https://doi.org/10.1177/00208523211039740

Sommerer L (2020) Personenbezogenes predictive policing. Nomos, Baden-Baden

SPIK (2016) System für Textanalyse zur Ermittlungsunterstützung. https://www.swisspoliceict.ch/getattachment/f007df9c-94ae-4617-9588-dec311ecfdb3/Kapo-ZH,-Unisys-IBM-Schweiz.aspx. Accessed 1 February 2022

Uchida CD (2014) Predictive policing. In: Bruinsma G, Weisburd D (eds) Encyclopedia of criminology and criminal justice. Springer, New York, pp 3871–3880

Ugwudike P (2020) Digital prediction technologies in the justice system: the implications of a 'race-neutral' agenda. Theor Criminol 24(3):482–501

Villasenor J, Foggo V (2019) Algorithms and sentencing: what does due process require? https://www.brookings.edu/blog/techtank/2019/03/21/algorithms-and-sentencing-what-does-due-process-require/. Accessed 12 February 2021

Yu C et al (2011) Crime forecasting using data mining techniques. In: IEEE 11th international conference on data mining workshops, 11 December 2011 Vancouver. IEEE: Danvers, pp 779–786. https://doi.org/10.1109/ICDMW.2011.56

Završnik A (2019) Algorithmic justice: algorithms and big data in criminal justice settings. Eur J Criminol. https://doi.org/10.1177/1477370819876762