

UC Irvine

UC Irvine Electronic Theses and Dissertations

Title

Digitized Criminal Justice: The Penal Field and Technology in the Digital Era

Permalink

<https://escholarship.org/uc/item/0tp2q94b>

Author

Rochow, Diego

Publication Date

2022

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA,
IRVINE

Digitized Criminal Justice: The Penal Field and Technology in the Digital Era

THESIS

submitted in partial satisfaction of the requirements
for the degree of

MASTER OF ARTS

in Social Ecology

by

Diego Rochow

Thesis Committee:
Assistant Professor Christopher Seeds, Chair
Assistant Professor Ana Muñiz
Chancellor's Professor Mona Lynch

2023

Table of Contents

	Page
List of Tables	iii
Acknowledgements	iv
Abstract of the Thesis	v
Introduction	1
1. Defining digital technologies	8
2. Criminal justice digitization: Police and courts	10
2.1. Predictive policing	11
2.2. Criminal courts	16
2.2.1. Risk and criminal justice	16
2.2.2. Digital technologies and criminal courts	19
3. The accounts of digital perils: An analytical model	24
3.1. The account of algorithmic datafication	26
3.2. The account of socio-digital biases	29
3.3. The account of juridical distortion	32
3.4. The why question: An analysis	35
4. Discussion: Towards an analytical expansion of research on criminal justice digitizing	39
4.1. Cultural representations, digital technologies, penal organizations	39
4.2. Institutional trajectories and penal digitizing	42
5. Conclusion	44
References	46

List of Tables

		Page
Table 1	Analytical model on the accounts of digital perils	26

Acknowledgements

I would like to thank my committee chair, Professor Christopher Seeds, for all his support and guidance during the development of this project. His academic work, analytical rigor, knowledge, and words of encouragement were a source of motivation and inspiration to complete this work. Our conversations around the topic of this thesis were crucial to shaping its structure and central arguments.

I would also like to express my gratitude to my committee members, Professor Ana Muñiz and Professor Mona Lynch, whose feedback and comments on this work have strengthened my interest in devoting my career to studying the impacts of technological developments on the foundations and functioning of the criminal legal system.

In addition, I thank Gonzalo García-Campo for his clarifying observations on early drafts of this thesis. I also want to express my deep appreciation to María Fernanda Muñoz, without whose care and understanding I would not have been able to be where I am. In the same way, I thank our cats, Akane and Chibi, for the joy they bring to our home.

Finally, the Chilean government and Fulbright Chile, through the fellowship ‘Beca de Doctorado Igualdad de Oportunidad (BIO) Fulbright-ANID 2018’, and the University of California, Irvine, provided financial support to conduct this research.

Abstract of the Thesis

Digitized Criminal Justice: The Penal Field and Technology in the Digital Era

by

Diego Rochow

Master of Arts in Social Ecology

University of California, Irvine, 2023

Professor Christopher Seeds, Chair

Over the last few years, punishment and new technologies studies have proposed novel concepts to describe digital technologies' impacts on the penal field. Currently, ideas such as *algorithmic justice* and *digital punishment* portray the use of artificial intelligence by penal agencies and the development of new citizen punishment forms on the internet. However, researchers have not yet systematically analyzed scholarship on criminal justice digitizing.

Through a literature review, this thesis introduces a conceptual model categorizing the ways in which scholars have studied the use of digital technologies in the penal system. This scheme shows the type of questions that researchers have addressed in investigating the penal implementation of digital technologies and establishes argumentative distinctions between these analyses. The thesis poses that studies on penal agencies' digitization have characterized this phenomenon from a critical perspective emphasizing its effective or potentially detrimental consequences for the functioning and foundations of criminal justice. The work conceptualizes this approach under the notion of the *accounts of digital perils* and divides the latter into a model

composed of three categories: the *account of algorithmic datafication*, the *account of socio-digital biases*, and the *account of juridical distortion*.

From the assessment of the *accounts of digital perils*, the thesis posits that scholars have evaluated from an especially critical prism the questions about *how* penal agencies employ digital technologies and *what consequences* their operationalization entails. At the same time, the work demonstrates that, in constructing the *accounts of digital perils*, researchers have yet to scrutinize with particular attention the reasons explaining the introduction and expansion of digital technologies in the penal system.

Consequently, the thesis examines the relevance of exploring why criminal justice organizations operationalize digital technologies and proposes strategies to address this question. It contends that evaluating the cultural representations surrounding the use of digital technologies in the criminal justice system and the institutional trajectories of penal digitization processes could contribute to generating new accounts around the digital future of the penal field.

Introduction

Whether with a political (Foucault, 1979) or penal (Rubin, 2016; Smith, 2003) qualification, the concept of technology has occupied a central place in the contemporary development of punishment studies. As an analytical construct, the notion of technology has constituted a basis for understanding the relations between the purposes of punishment and the historical forms of penal practices (Simon, 2013). Conceptually, it has allowed exploring how punitive techniques vary according to the cultural, political, economic, and social contexts in which state penal power deploys (Garland, 1990).

Despite the theoretical relevance of the idea of technology for analyses of penal transformations, the evaluation of the impacts of technological developments in criminal justice agencies has been, in historical terms, a relatively underexplored topic. However, the advent of 21st-century technological innovations and their effects on social relations have provoked some changes in this situation. Since the early 2000s, many scholars have examined how penal institutions' use of new surveillance and information technologies could expand the scope of social control methods and modify the significance of human knowledge in criminal justice management. For instance, Jones (2000) proposed a 'model of digital rule' to explain how the introduction of technologies such as electronic monitoring and CCTV cameras in the penal field expressed the consolidation of a social structure marked by the diffusion and inseparability of control practices throughout different institutional sites. Likewise, Franko (2004) postulated that by incorporating computing databases in criminal procedures, the binary ontology of digital language might come to replace the role of human judgment as one of the structuring axes of the penal system's functioning.

These analyses were attractive theoretical exercises in a period of uncertainty as to the scope and range of the changes that new technologies would entail for the structure and practices of criminal justice. They gave way to a research area whose study object was the emergence of new crime problems in the digital world. Nevertheless, they did not consolidate in a study line aimed at assessing the effects of technological developments' penetration in penal agencies.

Between the mid of the 2000s and the mid of the 2010s, studies on the connection between the digital and penal spheres centered on topics such as cybercrime, phenomena of virtual victimization, and digital security issues. This focus led some researchers to propose new fields of criminological specialization. Under ideas such as *cyber criminology*, an area devoted to studying the causes of crimes occurring in the cyberspace (Jaishankar, 2007), or *virtual criminology*, which aims to examine cybercrime and cyber-victimization through classical criminological knowledge (Bolton, 2014), scholars sought to circumscribe the analysis of digital penal phenomena to the domain of the internet. In these propositions, the central concern of scholars was to understand the patterns of crime activities digitization and, hence, they did not particularly consider how digitizing processes also impacted penal institutions and citizens' punishment and control practices. Nonetheless, in the last several years, an increasing number of authors have begun to promote the need to study further or directly have developed research addressing this latter phenomenon.

One first sign of this incipient shift is the idea of *digital criminology*. Different groups of authors have used this term to advocate for expanding the analyses of penal digitization beyond computer-related crimes through exploring the effects of digital tools in formal and informal crime control and the structure of the criminal justice system (Powell et al., 2018; G. Smith et al., 2017; Stratton et al., 2017). The framework of digital criminology proposes a broader basis than cyber or virtual criminology for studying penal digitizing.

Another sign of this turn is the emergence and progression of a set of works analyzing the development of new punitive experiences and phenomena linked to the digital world or evaluating the challenges that digital technologies suppose for criminology as a discipline. In this perspective, one can find the research by Lageson (2020; 2022) who have coined the expression *digital punishment* to depict how the pervasive availability of people's criminal records on the internet in the U.S. is shaping new stigmatization mechanisms that exceed the legal punishment's consequences and take place simultaneously both in digital and in physical spaces; the ethnographic investigation by Gurusami (2019) which characterizes the experiences of formerly incarcerated women when dealing with digital technologies as a *carceral web* since their criminal histories are embedded in time, virtual, and physical spaces so that for them it is practically unfeasible to become detached from their lives in prison; or the analysis by Chan and Bennett Moses (2016) on the consequences of using big data analytics in criminological research, in which they conclude that implementing this method must not lead to losing sight the identification of causes and mechanisms explaining both the origin of criminal behaviors and their control.

The last sign of this shift, and the most important one for this thesis' purposes, is the increasing concern of criminal justice and criminology researchers for scrutinizing the impacts of digital technologies in the penal system in general and penal agencies in particular. Either from a theoretical or empirical perspective, these studies explore how the implementation of big data analytics, artificial intelligence models, and digital algorithms for risk assessment in police departments (Brayne, 2017, 2018, 2020; Ferguson, 2017; Joh, 2014, 2016; Selbst, 2017) and criminal courts (Hannah-Moffat, 2019; Kehl et al., 2017; Mehozay & Fisher, 2019; Plesničar & Stubbs, 2017; Završnik, 2021) generate or could produce transformations in the practices and meanings associated with the state penal power's deployment in the digital era. The relevance of

this research body lies in that its approach seeks to shed light on those aspects of the connection between formal criminal justice and digitizing phenomena neglected by cyber and virtual criminology.

One way to examine this novel research line consists of systematically organizing its analyses in a model of theoretical categories. Although a model of analytical classification may seem a relatively basic exercise, it is a construct that scholars have not yet formulated when exploring criminal justice agencies' digitization. To date, this body of work has presented an inorganic character. Authors consider the ideas and findings of other researchers to reinforce their arguments or formulate new concepts, but they have not clearly delimited the connections or eventual contradictions between their theoretical postulates. Moreover, though in a recent paper, Lavorgna and Ugwudike (2021) pose that criminological and legal investigations on criminal justice digitization stand out for formulating oppositional frameworks to the automation of penal practices, their work is based on an evaluation and classification of abstracts. Hence, it does not address the theoretical structures and components of these studies in a particularized way.

Accordingly, the analytical features of this research area remain underexplored, and this turns out to be problematic when considering that the ways of thinking about criminal justice digitization may determine the public appreciation of this development. The socio-technical imaginaries (Jasanoff, 2015) of those who investigate penal digitization can shape collective representations influencing how people interpret the effects of this phenomenon in the social world (Jewitt et al., 2020). Thus, identifying the approaches through which researchers have studied criminal justice's digitizing processes could be a helpful exercise to explore the impacts of their analyses on audiences outside the academic field.

Through a literature review, this thesis introduces a conceptual model categorizing the ways in which scholars have studied the use of digital technologies in the criminal justice system. This scheme aims to show the type of questions that researchers have addressed in investigating the penal implementation of digital technologies and establish argumentative distinctions between these analyses. The thesis poses that studies on penal agencies' digitization have characterized this phenomenon from a critical perspective emphasizing its effective or potential detrimental consequences for the functioning and foundations of criminal justice. The work conceptualizes this approach under the notion of the *accounts of digital perils* and divides the latter into a model composed of three categories: the *account of algorithmic datafication*, the *account of socio-digital biases*, and the *account of juridical distortion*.

Drawing upon this model and evaluating the analytical structure of the distinct *accounts of digital perils*, the article posits that scholars have assessed from an especially critical prism the questions about *how* penal agencies employ digital technologies and *what consequences* their operationalization entails, formulating pessimistic projections on the eventual digital future of criminal justice. At the same time, the thesis demonstrates that, in constructing the *accounts of digital perils*, researchers have not evaluated the question around the reasons explaining the introduction and apparent expansion of digital technologies within the penal system with the same critical intensity. Instead, when exploring this inquiry, scholars usually provide uniform answers linking the use of digital technologies in criminal justice with the promises of improving the efficacy and efficiency of penal agencies, without especially problematizing the validity of these ideas to account for penal digitizing processes.

This way, the model of the *accounts of digital perils* primarily operates as an interpretative device clarifying the main conceptual aspects that scholars have scrutinized to describe and

theorize about criminal justice digitization. This typological model constitutes an instrument allowing for distinguishing the principal analytical characteristics of research on penal digitizing.

Consequently, and considering the general analytical structure of the *accounts of digital perils* that the model portrays, I examine the relevance of exploring why criminal justice organizations operationalize digital technologies from new perspectives. I contend that although the ideas of efficacy and efficiency make up coherent arguments to explain the deployment of penal digitizing processes, other conceptual alternatives could nuance the uniformity of this explanation both theoretically and empirically. Among them, the possibility that the reasons for which agencies introduce these tools experience transformations after their initial implementation stands out.

Finally, the thesis offers two complementary strategies to address the question of the reasons accounting for criminal justice digitizing. They consist of evaluating the cultural representations surrounding the use of digital technologies in the criminal justice system and the institutional trajectories of penal digitization processes. By deploying these approaches, studies on criminal justice digitizing could expand their explanatory potential in the near future, generating new accounts on the digital future of the penal field.

The thesis is organized as follows. Section one provides an operative definition of the expression *digital technologies* and other concepts associated with it for contextualizing their use in developing the work. It constitutes the terminological baseline underpinning the subsequent sections.

The second section presents an overview of the literature on penal digitization. It shows how this research line, focalized on the realities of the U.S., the U.K., and Australia, has

concentrated on analyzing two specific agencies: the police and criminal courts.¹ This section unveils the general argumentative structure of studies on penal agencies' digitization and makes up the backdrop for presenting the notion of the *accounts of digital perils* and their typological classification.

The third section synthesizes the investigations on the implementation of digital technologies in criminal justice institutions through the typological model around the *accounts of digital perils*, describes the ideas shaping each of its categories, and offers suggestions on how researchers could continue developing them. The last part of this section scrutinizes the class of questions that scholars have critically considered for structuring the *accounts of digital perils* and illustrates the relevance of evaluating the justifications of penal digitizing beyond effectiveness rationales.

In section four, the thesis explains the senses in which I conceptualize the ideas of cultural representations and institutional trajectories and discusses the utility of these approaches to delve into the question of why criminal justice agencies utilize digital technologies and project the digital development of the penal field.

The thesis concludes with a summary of its content and a general reflection on the importance of analyzing the digital present of criminal justice to understand the routes that penal digitization will follow in the near future.

¹ The geographical restrictions of these investigations can also be seen as theoretical and methodological limitations. Yet, I do not regard them as such since they suitably reflect the bounded character of penal digitizing processes and because I aim to describe the central diagnoses and arguments of scholars devoted to studying the use of digital tools in both organizations without paying particular attention to the local territorialities from where their analyses emanate.

1. Defining digital technologies

The emergence and evolution of digital technologies represent one of the biggest techno-social revolutions in contemporary human history. Their development is inextricably linked to advances in computing and telecommunications. The creation of personal computers and the internet, as well as the convergence between both innovations, were crucial to articulating the concept of digital technologies (Ceruzzi, 2013; Crook, 2013)

Rice, Yates, and Blejmar (2020) posit that digital technology presents four distinctive components. The first is digitization, the transformation of continuous physical signals used in analog artifacts to transmit information into discrete electric pulses disaggregating data through binary language exclusively composed of ones and zeros. The second component is computing, for digital data processing requires using computer platforms. Thirdly, there are microprocessors, which facilitate the integration of computers' data processing speed in devices like smartphones and laptops. In conjunction with digitization, this change has permitted producing, sending, and analyzing digital data by ever-smaller material objects (Ceruzzi, 2013; Lupton, 2015). Digital networking is the fourth component. It refers to information transmission networks that, like the internet, apply standardized protocols to simplify data exchange through virtual mechanisms yielding visualizable outcomes in physical devices.

Digital technologies constitute an umbrella term grouping objects such as personal computers and smartphones, telecommunications networks such as the internet, or tools that, like big data analytics or digital algorithms, base their functionalities on the interconnection between the processing and storage power of modern computers and digital networks. In this work, I use the expression *digital technologies* as a reference especially designating these latter developments.

I utilize concepts such as *algorithms*, *big data*, and *artificial intelligence* as sub specifications of the label *digital technologies*. Although I do not establish a sharp differentiation between all these expressions in the following sections, for conceptual clarity motives, it is necessary to specify some particularities relative to their meanings.

First, the notion of *algorithm* makes up a core element of computer science. It corresponds to the procedural rules coded in a programming language, composed of a finite quantity of symbols from a finite alphabet, allowing computing devices processing data to produce results in a finite amount of time (Rapaport, 2012). Alternatively, as Hill (2016, p. 58) points out, an algorithm is ‘a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions.’ The crucial point to consider for the development of succeeding sections is that the term *algorithms* or *digital algorithms* refer to the programming instructions through which digital technologies analyze data and bring about determined outcomes. I allude to the latter as *algorithmic results* or *algorithmic outcomes*.

Second, scholars discuss the perspectives from which one must depict the concept of big data. For some, it presents a fundamentally cultural character marked by how algorithmic power facilitates identifying patterns on vast amounts of data to create a mythological form of intelligence giving economic, legal, and social claims an aura of objectivity (boyd & Crawford, 2012). For others, and from a technical standpoint, big data is a statistical analysis technique. Three particular elements converge in its structuring: volume, velocity, and variety. Under this vision, big data is a mathematical procedure based on the power of digital computing to examine vast volumes of information through an extraordinary velocity of data processing and from an ample variety of separate institutional sources, which become unitary datasets through this technique. Due to these features, big data analytics can detect statistical associations at a speed and precision hard to

achieve through purely human intelligence (Lazer & Radford, 2017; Mayer-Schönberger & Cukier, 2013). From this definition, several studies have explored the relevance of big data in the criminological field (Brayne, 2020; Chan & Bennett Moses, 2016; Hannah-Moffat, 2019). Therefore, this thesis employs said expression alluding to the same meaning.

Lastly, despite expert research also debate about the possibility of describing artificial intelligence as a unitary analytical construct (McDaniel & Pease, 2021), to avoid theoretical complications, in this work, I use this term as follows. Artificial intelligence designates the capacity of digital technologies to operationalize mathematical logic on extensive datasets, producing results without the need for supervision and being able to create automatized algorithms that dispense with human programming (Russell & Norvig, 2010).

Against this conceptual backdrop, the next section delves into how scholars have analyzed the use of digital technologies in penal agencies.

2. Criminal justice digitization: Police and courts

The main developments that have attracted the attention of contemporary researchers studying criminal justice digitization are those related to the automation of decision making and the expansion of penal agencies' data processing capacities, such as digital predictive algorithms, artificial intelligence systems, and big data analytics. These technologies have been preponderantly implemented within and by two penal agencies, police departments, and criminal courts.²

² Some studies have investigated the operationalization of new technologies in prisons. Their general aim is to disentangle how the introduction of devices like smartphones and tablets in carceral settings generates transformations in the daily life of incarcerated people and the working routines of prison officers (Jewkes & Reisdorf, 2016; Kaun & Stiernstedt, 2020; Mufarreh et al., 2021). On the other hand, academic research on the use of algorithms and big data in prisons is still scarce. A few authors allude to the existence of digital algorithms supporting decision-making in parole proceedings, but they do not delve into this topic (Lavorgna & Ugwuđike, 2021; Plesničar & Stubbs, 2017). Likewise, in my literature review, I only detected one study particularly addressing the use of algorithms in the

The following two subsections summarize the visions of scholars analyzing the penal system digitization by addressing the use of big data and algorithms in policing and judicial penal practices.

2.1. Predictive policing

During the last decade, police departments, especially in the U.S., have intensified the incorporation of digital technologies in their work (Brayne, 2018). This phenomenon's prominence has led to a growing group of sociologists and criminologists specializing in the study of the so-called predictive policing. The body of work on this topic has expanded in an accelerated way in the last several years, so that investigations on police digitizing stand out by their increasing multiplicity.

Another relevant characteristic of this research line is its critical approach. Those who study predictive policing usually pose that the main effect of incorporating tools such as big data analytics and artificial intelligence in police work is the reproduction of the historical racial biases of law enforcement practices. The data with which digital technologies operate and the analysis techniques that these instruments employ in the policing context favor the enlargement of criminalization processes against black people. To sustain their critical analyses, scholars examine a set of recurring themes, presenting interpretations and conclusions whose argumentative composition tends to coincide. In particular, they focus on assessing how digital technologies

Pennsylvania prison system. In this work, the authors examine a digital tool facilitating the classification of incarcerated persons according to their risk levels for prisons' internal order and claim that the data and outcomes of this algorithm reflect and reproduce various racial biases (Massaro et al., 2022). Due to the features that research on digital technologies in prisons has presented, I opted to concentrate my analysis on the police and criminal courts. Essentially, this election has to do with the fact that scholars have explored their digitizing processes with greater detail than regarding prisons, especially emphasizing the assessment of tools that automate criminal justice.

expand the surveillance of disadvantaged populations and impact crime prevention. This section shows the forms in which researchers have characterized the use of digital tools in police departments from these considerations.

The connection between police surveillance expansion and implementation of new technological developments is one of the edges in studying predictive policing. Brayne's work (2017, 2018, 2020) is a reference on this subject. According to Brayne (2018), predictive policing operates by big data analytics to deploy two surveillance methods based on digital algorithms. On the one hand, in directed surveillance, police utilize historical crime data for training algorithms predicting when and where it is more likely that crimes occur; algorithmic outcomes determine the temporal and spatial extension of police surveillance. On the other hand, in dragnet surveillance, police departments use patterns-recognition algorithms on unparticularized data to generate samples of possible suspects in unknown perpetrator cases such that digital tools guide the development of this type of investigation. For Brayne (2020), these digitized ways of surveillance are problematic for their impacts on marginalized populations. Given that predictive algorithms operate on historical police data and policing concentrates traditionally on marginalized communities, the outcomes of big data analyses drive surveillance towards these groups. In her view, this focalization and police officers' racial biases and discretionary powers (Brayne & Christin, 2021) exacerbate criminalization processes against disadvantaged populations.

Similarly, Ferguson (2017) argues that big data policing constitutes an amplifying mechanism of invasive surveillance of black communities. Coining the idea of *black data*, Ferguson posits that police data with which predictive algorithms work reify law enforcement discriminatory practices. They obscure the latter in opaque computer functions and create legal and constitutional problems hard to solve through traditional law. Big data policing, in his view,

perpetuates the surveillance of poor neighborhoods of color through analyzing and reproducing black data. Complementing this analysis, Selbst (2017) contends that this effect also has discursive bases. Big data, predictive analytics, and artificial intelligence algorithms amplify discriminatory racial practices in the law enforcement realm since authorities represent them as tools for fabricating a purely technical and neutral social order, while in practice, patterns of biased policing broaden but, due to high-technology glare, they turn out less visible.

On the other hand, Joh (2016) poses that the problem of unfair police surveillance by big data links to the expansion of discretion in law enforcement. Digital data analysis facilitates tracing relations between people, objects, and locations that are not necessarily evident for traditional investigation techniques. These connections stem from opaque algorithmic processes in front of which the extant accountability and regulatory structures become ineffective, leaving to police discretionary powers the determination of big data surveillance privileged targets. In contrast to this diagnosis, empirically exploring the implementation of digital technologies in the U.K. police departments, other authors have detected practices differing from the argument on the negative intensifying of discretion. By interviewing police officers, Fussey and Sandhu (2022) established that these agents develop a *surveillance arbitration* role to decide the extension and aims of surveillance operatives. For these authors, law enforcement discretion does not only serve as an amplifying factor of policing, but on occasions, it can contribute to reducing the scope of surveillance practices. Officers may be wary of digital recommendations and limit the extent of operations based on personal decisions that disregard technological tools' suggestions. Thus, the argument on the issues of exacerbating police discretion by digital tools appears to require being contrasted with the lived experiences of officers operationalizing big data policing.

Usually, implementing digital technologies in police departments connects with the alleged potential of these tools to reduce crime levels. As Bennett Moses and Chan (2018) explain, algorithmic data analysis entails a promise of augmenting police forces' capacities to map when and where crimes will take place, which impacts the decisions determining officers unfolding in streets and neighborhoods. However, as the same authors note, this belief is not based on expert and independent assessments. It is often the result of media coverage about police digital innovations. For it, Bennett Moses and Chan have advocated for generating independent evaluations to understand further the consequences of predictive policing in crime prevention. Some scholars have assumed this challenge.

Analyzing extant quantitative evidence, Ridgeway (2018) systematically examined if big data and algorithmic techniques used by the U.S. police departments have helped to diminish crime levels. The author operationalized complex statistical procedures to show that though these tools have demonstrated some positive effects in the recovery of stolen vehicles, their claimed general benefits on reducing offending levels are far from materializing; predictive models have not yet brought about significant results in crime reduction. In a similar vein, Berk (2021) recently explored the statistical structures and processes of different police algorithms for crime prediction. As a result of his evaluation, Berk poses that comparing forecasting models does not yield conclusive results since the algorithms employed by each police department are excessively dissimilar and data-set dependent. Further, he points out that though some findings show a slightly higher capacity of predictive policing to forecast crimes compared to traditional policing practices, this margin of superiority is modest and limited to specific crimes. Therefore, the author concludes by holding that the advantages of predictive policing in terms of crime prevention depend more on police officers' abilities to interpret the outcomes of statistical tools than on technologies by

themselves. In their review of the theories and assumptions embedded in the use of predictive policing tools, Bennett Moses and Chan (2018) arrive at a similar conclusion.

Finally, it is worth underscoring that some authors like McDaniel and Pease (2021) argue that for evaluating the concrete efficacy of predictive policing, it is necessary to move away from its characterization as a homogenous construct. Instead, researchers should deploy particularized assessments of the effects of specific digital tools on crime rates in delimited contexts. In their view, by treating each predictive system as an independent instrument, it would be possible to clarify what predictive policing technologies are effective and what is not in crime reduction.

The detailed review of research on predictive policing reinforces the ideas posed at the beginning of this subsection. Scholars devoted to studying this phenomenon have critically scrutinized predictive technologies, remarking on their negative social impacts regarding surveillance expansion and unveiling the scarce evidence around their efficacy for crime prevention. These concerns raise more questions and doubts than convincing answers regarding the usefulness of digital technologies in policing.

If the available evidence indicates that these tools have a reduced incidence in controlling crime and produce adverse effects in socio-racial terms, why do police departments insist on their utilization? What factors could explain this situation? How do police authorities respond to in front of these findings and interpretations? In short, what justifications explain the origins and expansion of using digital technologies in policing?

The analytical model around the *accounts of digital perils* allows for advancing towards elucidating these issues. Although it does not provide direct answers to these questions, it facilitates identifying the analytical structure in which they insert. The third section of this thesis posits that penal digitizing research has not yet problematized in sufficient depth the question

around the reasons explaining the incorporation and expansion of digital technologies in the penal system, and this fact has limited its capacity to assess the vectors catalyzing or restricting criminal justice digitization processes. Thus, this typological model helps delimit the theoretical context in which the questions on the benefits and disadvantages of predictive policing could find responses.

However, before carrying out the analysis underpinning these ideas and arguments, it is crucial to consider the body of work focusing on the use of digital technologies in criminal courts. The following subsection presents a synthesis of these studies.

2.2. Criminal courts

Studies on criminal courts' digitization center on the incorporation and use of digital algorithms for risk assessment and supporting judicial decision-making throughout different stages of penal procedures. In research on this topic, evaluating the digitization of tools for risk assessment occupies a central place. The following subsection presents an overview of studies on risk in criminal justice. The subsequent subsection characterizes the modes in which scholars have explored the operationalization of digital technologies in criminal courts.

2.2.1. Risk and criminal justice

The introduction of risk assessment tools in criminal justice connects with the so-called 'avalanche of numbers' in society (Hacking, 1990). The constant measurement of people and their actions generated a form of social knowledge based on statistical logics of normality and deviance, which

opened up a new spectrum of possibilities to predict individuals' behavior probabilistically (Lynch, 2019).

In terms of practical evolution, criminological studies recognize four generations of instruments for risk assessment. The first generation consisted of clinical techniques with a holistic approach, in which professional psychologists evaluated the risk levels of individuals from personality tests; these methods started to be applied in the 1920s, and it was not until the mid-1980s that their use became relatively typical in the criminal justice system (Ávila et al., 2020). Second-generation tools developed between the mid-1980s and the beginning of the 1990s. Their distinctive feature was the inclusion of static risk factors, like criminal history, to produce immutable predictions of offenders' dangerousness (Andrews, 1989). The instruments of the third generation, operationalized during the 1990s, stood out for integrating dynamic variables, such as employment and education levels, to bring about changing risk scores which could be improved through personalized interventions. Lastly, in the fourth generation, whose development began in the late 1990s and continued in the 2000s, tools incorporated individual responsibility indicators related to subjects' responses to treatment interventions for establishing risk scores (Andrews & Bonta, 2010).

Currently, police departments, criminal courts, and parole boards utilize instruments of the second, third, and fourth generation to evaluate individuals' risk levels. Through questionnaires and demographic characterizations, the subjects' features are numerically parametrized and statistically analyzed to predict their degrees of dangerousness from quantified outcomes (Hyatt et al., 2011). In simplified terms, this is the sense in which scholars use the term actuarial techniques (Ávila et al., 2020). Their operationalization has been especially criticized for how statistical

correlations used to calculate the recidivism risk reproduce patterns of social disadvantage based on factors like class, gender, and race (Hannah-Moffat & O'Malley, 2007; Harcourt, 2006).

From a theoretical standpoint, arguably, the concept that best portrays the conceptual penal changes associated with the diffusion of actuarial logics in criminal justice is *the new penology* coined by Feeley and Simon (1992). For the authors, the implementation of risk-assessment instruments in criminal adjudication processes would have installed a form of penological knowledge in the structure of penal agencies that converted the classical conceptualization of crime. From a qualitative problem of individual moral motivations and deficiencies, it became an issue of statistical measurement of population groups, detection and prediction of risks, and efficient management of administrative resources. As a result, criminal justice would adopt prevention through incapacitation as its central goal in the new penology. Given its theoretical attractiveness, the idea of new penology has constituted one of the analytical lenses more employed by scholars devoted to examining the conceptual implications of incorporating risk assessment instruments in various criminal justice institutions, from juvenile justice to parole and incarceration (Brown, 2017).

The notion of risk is also theoretically linked to the expansion of penal practices focused on the management and control of population groups (O'Malley, 1992). Under this perspective, and as Simon (1988) noted in an early work, actuarial penal strategies involved significant turns in the ways of constructing penal knowledge and exercising penal power. The predictive goals of actuarial methods shaped penal techniques aimed at classifying people in contact with criminal justice according to the levels of risk they represent for the community. In this model, penal agencies do not seek to assess the moral or rational motivations of individuals but deidentify their

subjectivities to project their eventual future criminal activities in accordance with quantifying their personal traits.

Finally, it is worth noting that though the analyses around the idea of new penology and actuarial logics are suggestive theoretical constructs, empirical evaluations of their materialization in the penal field have yielded contradictory findings, which has led different authors (Brown, 2017; Cheliotis, 2006; Lynch, 1998; Miller, 2001) to pose arguments modifying Feely and Simon's (1992) original proposal.

This is the theoretical background in which studies on digital technologies and criminal courts have developed. In addition to scrutinize how digital tools modify the methods of risk assessments in judicial practices, these analyses employ the conceptual elements of the new penology framework to characterize the penal system's actuarial transformations in a scenario of increasing digitization. As the subsequent subsections show, this research line extends the theoretical bases of the new penology to explore the epistemic and normative impacts of criminal justice digitizing.

2.2.2. Digital technologies and criminal courts

One of the perspectives with which scholars have analyzed the use of digital tools in criminal courts seeks to unveil their effects on the epistemic structures of the penal system. Among the conceptual bases of this approach, the early work by Franko (2004, 2005) stands out. In her studies on criminal courts' implementation of computer databases, the author proposed a suggestive diagnosis about how these innovations could change penal knowledge's forms and nature. In her view, the binary language of databases transforms the traditional narrative knowledge of judging

processes in reasoning exercises merely aimed at producing outcomes. Under the ontology of the database, the question of *why* individuals involve in crime turns out irrelevant, the penal system operates by disarticulating individuals' subjectivity, and its aims become essentially actuarial. Though with nuances, these ideas have resonated in various contemporary analyses about criminal courts' digital automation.

According to Brownsword and Harel (2019), the introduction of artificial intelligence in criminal procedures has led some political authorities to deem this tool a potential replacement for legal rules in the penal system. The authors pose that the current design of digital algorithms does not seek to assist legal operators but replace them with automated decision-making processes for installing models of ex-ante preventive justice in place of ex-post punitive justice's structure. For the authors, in case of completing this transition, penal knowledge would lose its moral bases, and its legitimacy would depend on the efficacy of digital technologies to prevent crime through risk management. Also, in actuarial terms, Hannah-Moffat (2019) contends that the introduction of big data analytics in criminal courts represents a significant turn for the penal conceptualization of risk. Denominating the convergence of big data with risk assessment tools as a form of *algorithmic risk*, she holds that this phenomenon shapes an actuarial technique disconnected from the psychological tools customarily employed in judicial spaces to evaluate individuals' dangerousness. This method, moreover, entails a high degree of uncertainty regarding the accuracy of its risk predictions and presents a black box character. For Hannah-Moffat, the expansion of algorithmic risk systems in criminal courts may convert punitive interventions into intensified manifestations of algorithmic governance, a strategy in which human judgment is irrelevant to driving the penal system. Finally, Mehozay and Fisher (2019) argue that algorithmic risk assessment in criminal courts implies conceiving humanness from an a-theoretical and non-

reflexive perspective, to which they denominate the *algorithmic self*. This approach conceptualizes people as beings who lack self-correction ability. In these authors' view, the penal knowledge associated with the algorithmic self rejects the possibilities of redemption and rehabilitation for those in contact with criminal justice, facilitating the construction of a punishment system in which penal sanctions represent an exercise of pure state violence.

When investigating the insertion of digital algorithms in criminal courts, another set of scholars has examined the social and legal effects of this process. While the previous group centered on theorizing about the epistemic consequences of criminal justice digitizing, these researchers explore the practical consequences of this process.

In terms of social consequences, the works by Jefferson (2020) and Ugwudike (2020) are especially illustrative. Jefferson (2020) study the history of digital computing technology's upswing in the U.S. penal system and posits that its development constituted a means for enhancing mass racial criminalization. Digital technologies, with their cumulative effects on criminal courts' capacities for data storage and processing, contributed to expanding the racial biases of the war on crime. By speeding up the incorporation of young black men in the databases of different criminal agencies and easing their interconnection, digital computing acted as a central node to enlarge the adjudication processes in criminal courts. Hence, it facilitated the deployment of this penal strategy over racialized population. Jefferson deems penal digitization a racist subjugating strategy anchored in the power of technology. On the other hand, Ugwudike (2020) analyzes the racially disparate results of risk digital prediction technologies in the U.K. and U.S. courts. The author asserts that though these instruments formally satisfy race equality laws, they usually overpredict black people's recidivism rates. Per Ugwudike, this situation expresses how digital risk assessment tools potentiate the criminalization of racialized populations, an issue that she links to the

convergence between the discretionary power of the creators of digital technologies, problems of access to justice for black people, and historical judicial biases.

In the analyses of the legal impacts of digital tools, the work by Kehl, Guo, and Kessler (2017) about the implementation of risk-assessment algorithms in U.S. judicial decision-making constitutes a central edge. Synthetizing the content of public agencies' official reports, the authors point out that the use of digitized instruments in criminal proceedings has presented three central problems: the opacity of the data and rules with which risk prediction algorithms operate; their biased predictions when prognosticating without significant justifications a higher recidivism rate of black individuals compared to other populations; and the existence of a generalized uncertainty among judicial authorities as to whether these tools contribute to generating fair penal outcomes. Other authors have examined the juridical consequences of using algorithmic analyses in penal courts from these ideas.

For Završnik (2021), digital tools should only be supportive elements for judges' decision-making since they might increase the violations of defendants' constitutional rights. According to the author, the black box character of judicial algorithms can intensify the infractions to the principle of equality and the right to defense. On the one hand, if judges make decisions considering the algorithms' results and unknowing their eventual propensity to qualify specific social groups as more dangerous than others, equality is undermined. On the other hand, if defendants do not have the possibility of questioning how one court calculated the risk score that justifies the imposition of a punitive measure against them, the right to defense diminishes its validity. The author, thus, concludes with a call to carefully assess the algorithmic automation of criminal procedures. In a similar sense, Sourdin, Meredith, and Li (2020) explain that in the U.S. criminal justice system, the opacity of algorithmic tools for evaluating risk weakens defendants'

right to defense. Since those affected by penal measures emanating from the outcomes of algorithmic instruments cannot know the latter's functioning structure, they lack judicial means to question the origin of their penalties. The recent U.S. judicial case *State v. Loomis* reinforces this argument. As Liu, Lin, and Chen (2019) account for, in this decision, the Wisconsin Supreme Court determined that the proprietary character of the algorithm by which the tool COMPAS predicts the recidivism risk of individuals does not allow defendants to access its internal operative rules. Consequently, these scholars contend that the black box nature of algorithms in criminal courts is both technical and legal. The code of these digital tools is opaque, but the law protects this character. For Liu, Lin, and Chen, it implies underpinning the threats that algorithms represent to the principle of due process through legal norms.

Accompanying these analyses, Plesničar and Stubbs (2017) posit that the problems of incorporating digital algorithms in criminal courts' operations are also human and operative. Judges could progressively disregard how algorithmic outcomes reproduce judicial activity's biases when coming from data embodying criminal courts' historical patterns of judging. Lastly, it is important to mention that for authors like Bowling, Keenan, and Marks (2017), one of the central impacts of criminal courts digitization is the growing blurring of the frontiers between the phases of investigation and adjudication in penal proceedings. Since judicial decisions adopted with the support of digital tools respond to actuarial logics, their objectives resemble the functions of surveillance and prevention of policing without a clear justification for why the judiciary resorts to these developments.

The body of research assessing the unfolding of digital technologies in criminal courts' activities evaluates the extent to which these tools, and especially algorithms for risk prediction, shape a set of epistemic, normative, and procedural problems that destabilize or could alter the

habitual functioning structure of criminal justice. By considering current or prospective scenarios, authors analyze how algorithmic opacity and the use of digital technologies in penal proceedings can affect juridical principles such as equality and due process and disarticulate the narrative bases of penal knowledge. Critically, these studies contemplate with suspicion the utility of digital instruments in criminal justice settings.

3. The accounts of digital perils: An analytical model

In the previous section, I presented a summary of the approaches and ideas that researchers have developed when studying the implementation of digital technologies in police departments and criminal courts. These investigations assess the impacts of digitizing processes in said agencies in disaggregated ways. Despite these analyses sharing a critical perspective on the consequences of penal digitizing and coinciding at least partially in identifying the causes of these effects, they have not been organized in a systematic structure allowing to trace their descriptive and theoretical similarities and differences.

In what follows, I introduce a model of categories seeking to delineate such structure. The relevance of this typology lies in its potential to clarify the questions that the body of work on the use of digital tools in policing and criminal courts has formulated to explore this phenomenon, the answers and arguments researchers have developed to address them, and those aspects of penal digitization that scholars have not yet analyzed in sufficient depth. The question guiding this model's articulation is: How can one characterize, in general terms, the ways in which researchers have explained the impacts of digital technologies in criminal justice? This inquiry turns out significant when having in mind that scholars have not yet scrutinized the most significant

analytical features of this incipient research line and that its conceptual constructs can shape public imaginaries on penal practices digitizing.

Drawing from the prior section's content, I think the overall perspective with which scholars have studied the use of digital tools in penal agencies can be synthesized under what I call the *accounts of digital perils*. With this term, I allude to how the body of work on implementing digital technologies in the penal system, using distinct analytical approaches, has emphasized the detrimental, either actual or prospective, impacts of these tools on criminal justice's functioning and foundations. Under this prism, penal digitization appears as a disruptive phenomenon, with the potential for distorting the practices and normative pillars that legitimize the deployment of the state's punitive power. From this consideration, researchers have formulated arguments to criticize the automation of criminal justice, underscoring the significance of carefully examining its destabilizing effects.

The mutual feature of the *accounts of digital perils* consists of developing critical analyses, marked by a pessimistic view, of the consequences that entail operationalizing digital technologies in penal institutions. However, the penal spheres and domains scholars study as well as the discussions they pose to build their ideas, are not uniform. This quality is the basis for introducing a typological model around the *accounts of digital peril*. In particular, this schema is based on three categories. As I explained in the introduction, they are the *account of algorithmic datafication*, the *account of socio-digital biases*, and the *account of juridical distortion*. Table 1 synthesizes the conceptual model I propose. The following subsections delve into the content of its categories, identify some of their analytical shortcomings, and propose alternatives to face the latter.

Table 1. Analytical model on the accounts of digital perils

	Algorithmic Datafication	Socio-digital biases	Juridical distortion
Agency	Courts	Police and Courts	Courts
Orientation	Theoretical	Empirical / Theoretical	Theoretical
Practice	Decision making in penal procedures	Law enforcement and decision making in penal procedures	Decision making in penal procedures (emphasis in sentencing)
Peril	Denaturalization of epistemic nature	Amplification of social disparate outcomes	Distortion of normative bases
Core Argument	Language of database	Black box and historical practices and data	Black box
Referential Examples	Franko Aas (2004, 2007); Hannah-Moffatt (2019); Mehozay and Fischer (2020)	Brayne (2018, 2020), Jefferson (2020), Ugwudike (2020)	Kehl, Guo, and Kessler (2017); Završnik (2021)

3.1. The account of algorithmic datafication

This category includes those studies analyzing the consequences of the use of digital technologies for the epistemic nature of the penal system. Authors in this group concentrate on two critical aspects of traditional criminal justice: its narrative components and judicial decision-making. Especially considering the digitization of risk-assessment tools in penal procedures, scholars in this category pose that computerized databases, big data analytics, and algorithmic tools entail a peril of denaturalizing the human-narrative bases underpinning the decision-making processes of the judiciary.

Under the assumption that judges operate as agents constructing judicial narratives on defendants' lives to solve cases, these analyses argue that digitizing risk-assessment tools implies reducing the subjectivity of people in contact with the penal system to the numerical language of databases and algorithms. Accordingly, judging defendants by putting their actions in the broader context of their life conditions becomes an exercise of mathematical assessment. Algorithmic logics and objectified parameters constitute the dominant reasoning core by virtue of which judges determine the outcomes of criminal procedures and defendants' futures.

Research shaping the *account of algorithmic datafication* develops a set of arguments and conceptual labels aimed at remarking on how using digital tools in judicial decision-making may disintegrate the human subjective components that historically have characterized the penal system's functioning. For it, authors concentrate their efforts on explaining the epistemological perils associated with replacing judicial subjectivity and narrative assessments with algorithmic objectivity and statistical evaluations. In this approach, the main consequence of digitization processes is the disappearance of the narrative constructs from the criminal justice domain and the reduction of defendants' subjectivities to the binary code of digital data. Drawing upon this idea, scholars analyze the eventual transformations that digitizing criminal courts' practices may involve for the forms of penal knowledge and the meanings of punishment. The work by Franko (2004, 2005) on the epistemic roots of criminal justice and the ontology of databases, Hannah-Moffatt (2019) on algorithmic risk, and Mehozay and Fischer (2019) on the algorithmic self and the purposes of penal sanctions illustrate the argumentative line of this account.

The central peril in the *account of algorithmic datafication* is the possibility that digital technologies displace the relevance of human judgment to marginal positions within the criminal justice system. Extrapolating the reasonings of the authors representing this category, one could

even pose that a total *algorithmic datafication* of penal agencies might derive into a punishment system dominated by artificial intelligence and devoid of human components.

One of the main shortcomings of studies in this account lies in their high level of abstraction and the narrow contrast they establish between their theoretical postulates and the practical operationalization of digital technologies in penal agencies. The idea that algorithmic datafication can undermine the central place of narrative constructs in sustaining criminal courts' decision-making processes has a speculative theoretical character. Though it is a coherent and suggestive conceptual proposal, its empirical verification is still a pending challenge for those who have contributed to developing this account.

Indeed, some studies have detected that incorporating digital tools in criminal procedures can provoke effects dissimilar to the deformation of penal practices' narrative elements. For instance, in her study on the quantitative logics permeating the enforcement of sentencing guidelines in the U.S., which also inform the functioning of digital technologies, Lynch (2019) detects that the introduction of numeric language in courts does not generate a total replacement of legal actors' narrative constructions. Instead, mathematical assessments and outcomes enter into contact with the adversarial argumentative practices of criminal justice, giving way to the articulation of epistemic strategies in which penal operators seek to disentangle the meanings of quantitative language from the prevailing cultural paradigms in this institutional domain. From this prism, arithmetic reasoning does not eliminate human subjectivity, but the latter submits the former to its narrative rules. Moreover, in a recent work analyzing the implementation of a risk assessment software based on artificial intelligence in Wisconsin's criminal courts, Hartmann and Wenzelburger (2021) determined that the principal epistemic effect of this tool between practitioners consisted of reducing the uncertainty regarding the accuracy of their decisions.

According to the authors, legal operators conceived this algorithmic tool as a valuable reference point for underpinning their pronouncements, and it did not imply they dispense with their subjective judgments.

In consequence, one cannot obviate that ideas embedded in the *account of algorithmic datafication* make up interpretative possibilities that, if plausible, could not correspond to the practical reality of criminal justice digitization. The works by Lynch (2019) and Hartmann and Wenzelburger (2021) demonstrate how the operationalization of numerical algorithmic language in the penal system can adopt forms combining narrative elements and mathematical parameters, posing theoretical alternatives to rethink the foundations of the *account of algorithmic datafication*. By examining the arguments of the *account of algorithmic datafication* under an empirical perspective, researchers might reconsider the potential of digital technologies to completely replace the role of human judgment in criminal justice decision-making processes. This, in turn, could result in the construction of new accounts on the epistemic impacts of penal digitization.

3.2. The account of socio-digital biases

In this category, I group those studies underscoring how penal organizations' digital tools amplify and reproduce the criminal justice system's discriminatory biases, particularly in terms of race. Scholars in this line critically consider the use of digital technologies in police and courts' operations and its exclusionary impacts on marginalized black individuals and communities. Differently from the previous category, these authors do not posit evaluations about the global

epistemic effects of digital technologies' adoption on penal knowledge, but they emphasize the disparate consequences of these developments on the black population.

Drawing from a commitment to the notion of equality, research in the *account of socio-digital biases* pose that the operationalization of digital technologies in the penal system is a dynamizing factor of its discriminatory predispositions. These analyses, paying particular attention to the social effects of predictive policing and the insertion of predictive algorithms in criminal courts, contend that such tools facilitate the expansion of surveillance and social exclusion of black people. In this account, criminal justice digitization appears as an inherently discriminatory process stemming from two interconnected factors: penal agencies' historical data and practices and the black-box character of digital technologies' operative structures. The studies developed by Brayne (2017, 2018, 2020), Jefferson (2020), Ugwudike (2020), and Ferguson (2017) give form to this way of thinking about penal digitizing.

In the *account of socio-digital biases*, scholars conceive digital tools as means that expand the criminalization of black people and link this consequence to the reproduction of punitive practices' historical racial biases through digital data. Further, these researchers argue that the lack of transparency on the production and utilization of information in algorithmic analyses is an amplifying factor of racial discrimination. Criminal justice digitization in this approach, especially when considering the scarce evidence on the effectiveness of tools such as algorithms of predictive policing in crime prevention (Bennett Moses & Chan, 2018; Berk, 2021; Ridgeway, 2018), entails a generalized peril of intensifying the penal system's socio-racial biases.

As noted in subsection 2.1 on predictive policing, one of the peculiar features of penal digitizing processes is the mode in which their deployment occurs and seems to settle over time despite the evidence regarding their preventive and deterrent utility being not particularly decisive.

Instead, as one can extract from the *account of socio-digital biases*, analyses of the practical consequences of this phenomenon substantially emphasize its harmful effects on marginalized communities and people. But, at the same time, both analytical domains usually develop in a disconnected way. That is, while some studies concentrate on illuminating the problems of penal digital technologies in terms of their technical efficacy, other investigations remark on their disparate social outcomes, without any of them establishing clear and specific links between their corresponding findings.

Particularly in the case of research structuring the *account of socio-digital biases*, this disconnect may limit their persuasive capacity. If the objective of their authors is to articulate analyses aimed at questioning penal practices digitizing, the identification of their detrimental racial impacts and the explanation of the factors producing the latter can be insufficient arguments to convince authorities and citizenry of the need for reconsidering the convenience of incorporating the use of digital tools in criminal justice. This is so since examining penal digitization's consequences is an exercise that does not imply by definition an evaluation of the purposes and likely benefits of this phenomenon.

One of the avenues by which studies shaping the *account of socio-digital biases* could reinforce their analytical structure and critical potential is the possibility of connecting their findings and conclusions with the investigations emphasizing the limitations of digital tools to contribute to controlling and reducing crime. By showing that the positive effects of penal digitization on crime prevention tend to be scant and that its negative racial impacts exacerbate social discrimination patterns, the arguments justifying this account could acquire greater expressive and persuasive force. For sure, materializing this strategy will depend on the visions and perspectives of those who have participated in devising the *account of socio-digital biases*.

However, I think that exploring this proposal would help complement its postulates, providing them additional critical weight.

3.3. The account of juridical distortion

Under this category, research remarks on the perils digital technologies can imply for the criminal justice system's internal functioning, the principles informing it, and defendants' rights and constitutional safeguards. With some exceptions, most authors in this group develop theoretical exercises describing diverse juridical issues associated with the implementation of digital algorithms for risk prediction in criminal courts. Their analyses underscore how algorithmic tools and artificial intelligence models' black-box nature produce judicial scenarios in which concretizing normative standards such as due process or the equality of defendants before the law is an elusive goal.

In this perspective, algorithmic opacity constitutes a conceptual and practical barrier to realizing the ideals of justice legitimizing the penal system. The short technical and procedural transparency regarding how judicial algorithms generate their outcomes and the way in and the extent to which judges consider the latter in making decisions distorts the theoretical validity of principles like due process or defendants' rights to defense. For authors in this category, the lack of knowledge around the operative structures of these tools impedes assuming that their implementation aligns with the normative foundations of criminal justice. Therefore, from a legal and institutional standpoint, these researchers have critically evaluated the juridical impacts of penal digitizing processes.

Through a theoretical prism and utilizing secondary sources, scholars in this group aim to evidence the practical and normative disruptions that an eventual totalizing judicial automation, in connection with algorithmic opacity, may bring about. Their analyses express a concern with the possibility that algorithmic criminal justice continues its expansion, undermining the legal principles seeking to moderate the deployment of the state penal power. Research by Kehl, Guo, and Kessler (2017), Sourdin, Meredith, and Li (2020), and Završnik (2021) portray the central argumentative lines of this approach.

The *account of juridical distortion*, in sum, characterizes the penetration of digital technologies in criminal courts from its potential to alter some of the most meaningful normative bases of the penal system's workings. To sustain their arguments, scholars link this issue with the lack of transparency and knowledge, both internal and external, concerning how digital algorithms for risk prediction and assessment produce their outcomes. This account focuses on constructing theoretical arguments that shed light on penal digitization's juridical perils.

The construction of the *account of juridical distortion* coincides with one characteristic distinction of juridical research on justice digitization in the realm of public law. As Livingston (2021) explains, scholars in this legal area have examined the incorporation of digital technologies, and especially the case of artificial intelligence, in public institutions taking into account two differentiated analytical domains. On the one hand, the study of the internal impacts of judicial digitization focused on understanding how legal operators and professionals use and conceptualize new technologies. On the other hand, the assessment of its external impacts focused on the transformations that technological developments provoke in the relations between these agencies and society. Considering this conceptual division, one can note how the studies on penal digitizing in the *account of juridical distortion* have a similar orientation to the latter perspective, as their

analytical structure concentrates on scrutinizing the impacts of digital technologies on the normative bases marking the social legitimacy of criminal courts' practices. In turn, this association unveils that the approach of the *account of juridical distortion*, with its emphasis on the legal effects of penal digitizing, possesses a hybrid nature mixing elements of criminological research and legal studies on digitization phenomena.

Finally, in the same way as the other *accounts of digital perils*, this account also presents some limitations. In particular, its investigations have a restricted scope to explain, from robust empirical findings, the specific functional mechanisms through which implementing digital technologies in penal settings generates normative distortions.

Studies shaping the *account of juridical distortion* use hypothetical assumptions or specific cases of the U.S. judicial reality to identify the normative problems associated with penal digitizing processes and link these issues with algorithmic opacity. Then, though this theoretical exercise yields likely results in argumentative terms, they have not been subjected to evaluations aimed at determining its actual and generalized correspondence with criminal justice digitization in action, both in the U.S. context and in other jurisdictions. This does not mean that the reasonings around the black box character of penal algorithms and its juridical distortive consequences are neither convincing nor credible. Rather, it implies arguing that the logical bases of the *account of juridical distortion* should be supplemented with studies whose specific purpose is to test the variability of degrees in which criminal courts' digitizing affects principles such as due process and equality. New research adopting this perspective could enrich the empirical bases of this account.

3.4. The why question: An analysis

The *accounts of digital perils* allow for detecting a peculiar feature of the way in which scholars, to date, have explored the impacts of implementing digital technologies in the criminal legal system. Its analytical categories express a notorious concern with the future of criminal justice. The descriptive elements and argumentative roots of the accounts on *algorithmic datafication*, *socio-digital biases*, and *juridical distortion* seek to warn of the prospective risks that digitization processes imply for the narrative epistemic nature, the socio-racial effects, and the normative bases of the penal system.

Faced with the opacity of algorithmic black boxes and the epistemic, social, and legal problems associated with this feature, scholars have opted to take a skeptical and cautious position. By examining the impacts of digitization in criminal justice, their analyses have adopted an orientation that emphasizes the adverse effects of this process. The model around the *accounts of digital perils* contributes to tracing the type of analytical structures in which this perspective inserts, and, consequently, it helps clarify the conceptual bases of the latter. Thus, this typology constitutes an interpretative device to shed light on the relations between the research questions scholars have explored when studying criminal justice digitizing and the standpoints that they have deployed to answer these inquiries.

The categorization of the *accounts of digital peril* shows that studies on criminal justice agencies' digitization seek to answer two relatively delimited questions. On the one hand, *how* do police departments and criminal courts use digital technologies? On the other hand, *what consequences* do these using forms entail? Concentrating on these aspects of penal digitization, authors have defined a primary framework to understand the impacts of this phenomenon.

By addressing how penal organizations use digital technologies, scholars have shed light on the instrumental characteristics of their implementation, the apparent trust in algorithmic objectivity due to its mathematical foundations, and the scarce critical reflexivity of agencies when incorporating these developments in their organizational configurations. Then, the valuations and arguments on the consequences of penal digitizing processes constitute derivations of the findings linked to the question of how criminal justice agencies employ digital tools. The *accounts of digital perils* and their emphasis on the issues of discrimination and normative and epistemic distortions that digital technologies provoke in criminal justice settings directly correlate to problematizing their current ways of operationalization. Under this vision, the negative critical position of scholars devoted to analyzing criminal justice digitization is an outcome of the research questions and analytical structures from which they have studied this phenomenon. These factors are the bases that determine their apprehensions regarding the prospective unfolding of digital tools in criminal justice organizations.

The model associated with the *accounts of digital perils*, in this sense, possesses multiple relevant edges. Firstly, it illuminates the distinct ways in which scholars have studied the implementation of digital technologies in the penal system, considering the differences between the account of *algorithmic datafication*, the account of *socio-digital biases*, and the *account of juridical distortion*. Secondly, it allows for identifying the analytical structure that these accounts share in terms of research questions and how the latter connects with the critical perspective currently characterizing studies on penal digitizing. Thirdly, it sheds light on those questions on criminal justice digitization that researchers have not yet incisively problematized and whose detailed analysis could contribute to expanding this study line's scope and analytical depth. The following paragraphs address this last point.

The inquiry on why penal agencies employ digital technologies has not been analyzed with the same critical intensity that researchers have deployed when examining these tools' forms of use and impacts on criminal justice organizations. As can be extracted from the model on the *accounts of digital perils*, scholars articulate different critical perspectives and answers in constructing their analyses around the latter subjects. However, when exploring the reasons for which penal institutions have resorted to technological innovations such as artificial intelligence and big data analytics, their assessments tend to be uniform and present a less critical emphasis. In particular, researchers usually associate the justifications of penal digitization with the ideas of efficacy and efficiency. Some examples illustrate this idea.

In the studies on predictive policing and algorithmic risk assessment in criminal courts, authors contend that penal agencies have implemented digital technologies in their practices of investigation and judging since these tools constitute means that promise to increase their levels of organizational efficiency and material effectiveness in crime reduction. The former, because analytical techniques like big data, would contribute to improving the allocation of material and human resources by facilitating the identification of those institutional areas in which agencies develop inefficient customs in terms of costs and benefits. In the case of police, this idea translates into the redistribution of officers in the streets from the results of algorithmic analyses (Brayne, 2020), while in the case of courts, it implies the introduction of digital devices to multiply legal actors' work productivity (Franko, 2004, 2005; Završnik, 2021). The latter, for both the alleged objectivity of digital data analysis and the optimization of institutional efficiency, would converge in producing more refined penal outcomes during criminal proceedings, which ultimately would determine possible reductions in crime rates because of the deterrent and preventive effects of punitive measures (Brayne, 2018; Franko, 2004, 2005; Jefferson, 2020; Završnik, 2021).

This standard explanation is debatable for at least two reasons. On the one hand, authors mention it as a complementary element of their analyses. They allude to the notions of efficiency and efficacy as contextual information reinforcing the sense of their findings and conclusions or seeking to facilitate the concatenation of their arguments. Accordingly, this justification has not been subjected to forms of critical scrutiny in which the question around the reasons explaining penal digitizing occupies a central place in the analytical structure of investigations. The peripheral position of this question and its eventual answers in the studies on criminal justice organizations' digitization has restricted the odds of exploring the factors constraining or favoring this process.

On the other hand, even if one accepts the discourse of efficacy and efficiency as valid reasoning to explain penal agencies digitizing, such an argumentative strategy has a partial character. This justification clarifies why criminal justice organizations introduce digital technologies in their daily functioning in a primary phase. Nevertheless, it does not account for why, once this establishment occurs, agencies continue to utilize digital tools nor why penal digitization seems to be developing a gradual expansion process. Further, if one assumes that the penal system operates as a social domain in which diverse economic, political, and cultural forces coalesce to shape its objectives and operative mechanisms (Garland, 1990), penal agencies can be deemed translational spaces in constant transformation. This way, the reasons justifying the insertion of determined technological developments in the formal penal sphere are not necessarily the same as those supporting the proliferation of their use throughout criminal justice institutions. These arguments bolster the need to delve into why penal agencies employ digital technologies.

Based on this analysis, the following section proposes two interconnected strategies to explore criminal justice digitizing processes. In them, the reasons underlying this phenomenon constitute a central study object.

4. Discussion: Towards an analytical expansion of research on criminal justice digitizing

Problematizing the question of why criminal justice organizations use digital tools is an important exercise as it may enhance the analytical depth of research on penal digitizing. It can illuminate how the justifications for operationalizing these instruments connect with diverse constitutive elements of the penal system. Nonetheless, as relevant as examining this question is the determination of the study objects and strategies that one takes into account to explore it. This is so since analytical entities and approaches are structuring factors of the path leading to detecting specific findings and formulating particular interpretative conclusions (Canguilhem, 2005 [1968]; Mahoney, 2000).

Against this backdrop, what analytical strategies could help further understand the reasons for criminal justice agencies' digitization? Two approaches that could be especially instructive for it consist of analyzing the cultural representations surrounding the use of digital technologies in penal organizations and articulating the institutional trajectories of penal digitizing processes. In what follows, I spell out the senses in which I conceptualize each of these strategies and explain how they can help expand the understanding of why penal institutions digitize their practices.

4.1. Cultural representations, digital technologies, penal organizations

The idea of scrutinizing the cultural representations around digital technologies in criminal justice points toward exploring the penal conceptualizations of these tools on multiple levels and how these interpretations link with the reasons explaining their operationalization and, on occasions, also determine their using forms.

At the level of penal actors and their professional field, some of the studies in the *accounts of digital perils* have documented how criminal justice operators do not univocally value the usefulness of tools such as big data analytics and artificial intelligence in their labor activities. For instance, in the case of predictive policing, Brayne (2020) and Brayne and Christin (2021) have detected that officers do not show blind confidence in the potential of algorithmic outcomes to predict crime. Rather, the decision to use these technologies in daily policing depends on the extent to which agents consider that algorithms contribute to improving the effectiveness of their control practices. In this evaluation, aspects like the place that officers occupy in the police hierarchy, levels of labor experience, age, and cultural valuations of the advantages of technological innovations for social development, constitute variables determining the propensity of police agents to incorporate digital tools in their daily work routines.

Likewise, in the realm of criminal courts, the work by Lynch (2019) regarding the penetration of quantitative logics in sentencing practices posits a significant consideration on the relevance of examining this phenomenon in light of the cultural paradigms associated with the judicial activity. In effect, Lynch's analysis demonstrates that the conceptualization of sentencing guidelines in the U.S. courts results from translation processes in which the mathematical reasoning converges with the confrontational culture of legal actors to bring about particular interpretations of the meanings of quantitative language. Cultural factors, in this sense, and concerning digital technologies, operate as translational vectors on the quantitative logics that these tools embed and operationalize, generating contextual understandings from which penal agents determine the consequences of criminal procedures.

Finally, at the social level, several anthropological studies have underscored how the conceptualizations of *the digital* are not static nor allude in all scenarios to homogeneous ideas. In

rural Bangladesh, for example, communities link digital technologies to symbols of elegance and social sophistication (Huang, 2018), while in India, some social groups reject the utilization of these devices as they represent occidental menaces to their indigenous local identities (Nair, 2021). These conceptions reinforce the idea that digital technologies' value and use forms respond to the cultural contexts in which they deploy. Cultural representations constitute one of the bases on which it is possible to explore the reasons motivating individuals, institutions, and communities, to employ different digital tools.

These analyses show that cultural representations around technology are factors conditioning the digitizing processes. Consequently, assessing the forms in which penal agents think about digital tools in their professional fields, how penal organizational cultures impact the structuration of these conceptions, and even their variations according to socio-geographical contexts become mechanisms to explore why criminal justice agencies like the police and courts have operationalized and continue recurring to digital technologies.

Studying penal cultural representations of these innovations at different levels should shed light on the rationales underpinning their introduction and eventual expansion in and between organizations. Conceptualizations regarding the utility or futility of these instruments in penal actors' daily work and the institutional culture of agencies should determine distinct levels of intra-organizational and inter-organizational acceptance or rejection. In turn, these factors should resonate in the scope and depth of penal digitization phenomena. By analyzing the cultural elements embedded in the penal implementation of digital technologies, studies on this topic would encounter a fertile terrain to scrutinize the reasons explaining the use of these tools in criminal justice. Thus, explicitly investigating the cultural components of penal digitization may constitute a productive strategy to delve into the justifications behind this phenomenon.

4.2. Institutional trajectories and penal digitizing

The strategy of investigating the institutional trajectories of criminal justice digitization allows addressing a set of questions on the paths through which digital technologies have navigated within penal institutions and the eventual communication routes by which digitization has moved from one agency to another. In straightforward terms: What operative areas of police departments and what stages of criminal procedures were the first in incorporating digital tools into their functioning? How did this introduction impact the organizational structures of these agencies? What factors or considerations may explain the extension in the use of digital technologies towards other sectors of police offices or phases of criminal proceedings after their initial insertion? Then, when noting the digital development of both agencies: What are the institutional connections between their digitization? When police departments adopted digital technologies, did criminal courts subsequently imitate them? Did both agencies operate through different and disconnected digitizing designs? Is it possible to describe criminal justice digitization as a continuous or discontinuous process when taking into account that the agencies comprising the penal system are dissimilar in their institutional configurations and purposes?

All these questions still do not have well-defined answers in criminal justice and digital technologies studies. One potential route to explore them is reconstructing the stages through which penal digitization has been deployed in specific penal institutions and establishing the possible connections between the digital developments of the distinct organizations composing the penal system. This strategy would allow raising an explanatory diagram to illustrate and make visible how the introduction of digital technologies in one agency occurs, what happens after this

initial phase, and how, possibly, the expansion of these tools from one organization to another takes place. This is the sense in which I conceive the notion of institutional trajectories.

Using this approach, analyzing the reasons behind digitization unfolding becomes an identification and association exercise. Tracing the adoption paths of digital tools in different agencies would facilitate detecting the general or particularized argumentative structure of their implementation within the criminal justice system. This strategy would contribute to determining whether the reasons by which one penal agency starts a digitizing process maintain when it enlarges within the same organization or if, instead, said justifications change. At the same time, it would allow establishing if the rationale underlying the incorporation of digital tools in one particular institution also reproduces in the digitizing of agencies with unlike functions in penal procedures. In short, this type of evaluation would provide a robust analytical baseline for distinguishing and interpreting the reasons behind the introduction and gradual growth of digital technologies in the penal system, both in terms of individual agencies and inter-organizational links.

In the sociology of punishment, some have recently proposed to employ historical institutional theories to explain how penal changes occur and develop at the meso-level of criminal justice agencies (Rubin, 2021). However, the idea of analyzing the institutional trajectories of penal digitization points here in a somewhat different direction. To portray the vias of institutional adoption and extension of criminal justice digitizing aims to situate this phenomenon in the context of the practices and legal regulations that have facilitated its development through specific arrangements (Garland & Young, 1983) in the penal system. Articulating these schemas facilitates conceptualizing the forms of the material and cultural infrastructures (Willis, 2005) that have enabled the rise of penal digitization processes. These infrastructures hold penal meanings and

practices through validation processes based on recognition, corroboration, or resonance (Seeds, 2022), and literature on criminal justice digitizing has not specifically determined what the infrastructural bases supporting the use of digital tools in criminal justice are.

By graphing the institutional trajectories of criminal justice digitizing, researchers could scrutinize with a high level of granularity the classes of infrastructures that have permitted the introduction and apparent expansion of digital technologies in penal agencies, accounting for, in turn, the reasons underpinning this development. Analyzing penal digitization from contextual-institutional elements at the level of particular criminal justice organizations and the relations of agencies could contribute to understanding what connections exist between the infrastructural bases and reasons that have supported this phenomenon in institutional terms. Further, this strategy would help determine the explanatory capacity of the efficacy and efficiency discourse, establishing if such argument requires to be complemented or nuanced.

In analyzing the reasons underlying criminal justice organizations' digitizing processes by the study of the cultural representations and institutional trajectories associated with this penal development, scholars could generate investigations expanding the analytical scope and depth of research on this topic. Perhaps, by these strategies, we could delineate a comprehensive map to explore the future of the penal field beyond the *accounts of digital perils*.

5. Conclusion

This work has proposed an analytical model around the *accounts of digital perils* to explain the critical approaches with which researchers have analyzed the effects of penal digitizing processes. In introducing this typology, composed of the *account of algorithmic datafication*, the *account of*

socio-digital biases, and the *account of juridical distortion*, I presented the arguments underpinning these categories, showing as well, a series of aspects that scholars could consider for developing them further.

Drawing on this model, I contended that the construction of the *accounts of digital perils* and their pessimistic projections on the digital future of the penal field stem from the critical consideration of two interrelated research questions. On the one hand, the question related to how penal agencies use digital technologies. On the other hand, the question around the consequences involving the operationalization of these tools. In describing this configuration, I posed that, unlike these questions, the inquiry on the reasons explaining penal digitization has not been studied with the same critical emphasis by researchers. This, for they have deemed the notions of efficacy and efficiency as uniform explanatory substrates to respond to it. Then, I accounted for that problematizing why these organizations employ digital tools beyond the ideas of efficiency and efficacy is a relevant exercise in light of the translational character of the penal system. Finally, the work argued that studying the cultural representations associated with and institutional trajectories of penal digitization might constitute valuable prospective strategies to analyze the reasons explaining this phenomenon.

As a conclusive note, it is worth mentioning that this thesis has aimed to organize and characterize the analysis lines that research on criminal justice digitizing has presented to date. As such, the model on the *accounts of digital perils* and the proposals I have posited have an interpretative purpose and, in no case, a prescriptive one.

Moreover, it is relevant to note that penal digitization is an ongoing process, and it allows for constantly formulating new questions on its development. For instance: How do prisons operationalize, or will use, digital algorithms and big data? Will police and criminal courts'

digitizing give way to prisons' digitization? What will be the role of new digital technologies such as the internet of things in the penal system? In sum, how will the digital future of criminal justice look? At this moment, I do not have solid answers to any of these questions. Nonetheless, I think our possibilities of addressing them with precision will depend on the deepness with which we understand the penal field's present digital history. Ultimately, this thesis has sought to promote building said history.

References

- Andrews, D. A. (1989). Recidivism is predictable and can be influenced: Using risk assessments to reduce recidivism. *Forum on Corrections Research*, 1, 2–4.
- Andrews, D. A., & Bonta, J. (2010). *The Psychology of Criminal Conduct*. Routledge.
- Ávila, F., Hannah-Moffat, K., & Maurutto, P. (2020). The seductiveness of fairness: Is machine learning the answer? – Algorithmic fairness in criminal justice systems. In *The Algorithmic Society*. Routledge.
- Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society*, 28(7), 806–822. <https://doi.org/10.1080/10439463.2016.1253695>
- Berk, R. A. (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. *Annual Review of Criminology*, 4(1), 209–237. <https://doi.org/10.1146/annurev-criminol-051520-012342>
- Bolton, A. (2014). Virtual Criminology. In *The Encyclopedia of Theoretical Criminology* (pp. 1–3). John Wiley & Sons, Ltd. <https://doi.org/10.1002/9781118517390.wbetc092>
- Bowling, B., Keenan, C., & Marks, A. (2017). Automatic Justice?: Technology, Crime, and Social Control. In *The Oxford Handbook of Law, Regulation and Technology* (pp. 706–730). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199680832.013.32>
- boyd, danah, & Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication & Society*, 15(5), 662–679. <https://doi.org/10.1080/1369118X.2012.678878>
- Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>
- Brayne, S. (2018). The Criminal Law and Law Enforcement Implications of Big Data. *Annual Review of Law and Social Science*, 14(1), 293–308. <https://doi.org/10.1146/annurev-lawsocsci-101317-030839>
- Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.

- Brayne, S., & Christin, A. (2021). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*, 68(3), 608–624. <https://doi.org/10.1093/socpro/spaa004>
- Brown, M. (2017). The new penology. In A. Brisman, E. Carrabine, & N. South (Eds.), *The Routledge Companion to Criminological Theory and Concepts* (pp. 459–462). Routledge.
- Brownsword, R., & Harel, A. (2019). Law, liberty and technology: Criminal justice in the context of smart machines. *International Journal of Law in Context*, 15(2), 107–125. <https://doi.org/10.1017/S1744552319000065>
- Canguilhem, G. (2005 [1968]). The Object of the History of Sciences. In G. Gutting (Ed.), *Continental Philosophy of Science* (pp. 198–207). Oxford: Blackwell Publishing.
- Ceruzzi, P. (2013). The Historical Context. In *The SAGE Handbook of Digital Technology Research* (pp. 9–25). SAGE Publications Ltd. <https://doi.org/10.4135/9781446282229>
- Chan, J., & Bennett Moses, L. (2016). Is Big Data challenging criminology? *Theoretical Criminology*, 20(1), 21–39. <https://doi.org/10.1177/1362480615586614>
- Cheliotis, L. K. (2006). How iron is the iron cage of new penology?: The role of human agency in the implementation of criminal justice policy. *Punishment & Society*, 8(3), 313–340. <https://doi.org/10.1177/1462474506064700>
- Crook, C. (2013). The Field of Digital Technology Research. In *The SAGE Handbook of Digital Technology Research* (pp. 26–40). SAGE Publications Ltd. <https://doi.org/10.4135/9781446282229>
- Feeley, M. M., & Simon, J. (1992). The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*. *Criminology*, 30(4), 449–474. <https://doi.org/10.1111/j.1745-9125.1992.tb01112.x>
- Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.
- Foucault, M. (1979). *Discipline and Punish: The Birth of the Prison*. Vintage Books.
- Franko, K. (2004). From narrative to database: Technological change and penal culture. *Punishment & Society*, 6(4), 379–393. <https://doi.org/10.1177/1462474504046119>
- Franko, K. (2005). *Sentencing in the Age of Information: From Faust to Macintosh*. Routledge-Cavendish. <https://doi.org/10.4324/9781843146346>
- Fussey, P., & Sandhu, A. (2022). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, 26(1), 3–22. <https://doi.org/10.1177/1362480620967020>
- Garland, D. (1990). *Punishment and Modern Society: A Study in Social Theory*. Clarendon Press.
- Garland, D., & Young, P. (1983). Towards a Social Analysis of Penalty. In D. Garland & P. Young (Eds.), *The Power To Punish. Contemporary Penalty and Social Analysis* (First Edition, pp. 1–36). Heinemann Educational Books.
- Gurusami, S. (2019). The Carceral Web we weave: Carceral citizens' experiences of digital punishment and solidarity. *Punishment & Society*, 21(4), 435–453. <https://doi.org/10.1177/1462474518790237>
- Hacking, I. (1990). *The Taming of Chance*. Cambridge University Press.
- Hannah-Moffat, K. (2019). Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. *Theoretical Criminology*, 23(4), 453–470. <https://doi.org/10.1177/1362480618763582>
- Hannah-Moffat, K., & O'Malley, P. (2007). *Gendered Risks*. Taylor and Francis. <https://doi.org/10.4324/9780203940556>

- Harcourt, B. E. (2006). *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. University of Chicago Press. <https://doi.org/10.7208/chicago/9780226315997.001.0001>
- Hartmann, K., & Wenzelburger, G. (2021). Uncertainty, risk and the use of algorithms in policy decisions: A case study on criminal justice in the USA. *Policy Sciences*, 54(2), 269–287. <https://doi.org/10.1007/s11077-020-09414-y>
- Hill, R. K. (2016). What an Algorithm Is. *Philosophy & Technology*, 29(1), 35–59. <https://doi.org/10.1007/s13347-014-0184-5>
- Huang, J. Q. (2018). Digital aspirations: ‘Wrong-number’ mobile-phone relationships and experimental ethics among women entrepreneurs in rural Bangladesh. *Journal of the Royal Anthropological Institute*, 24(1), 107–125. <https://doi.org/10.1111/1467-9655.12754>
- Hyatt, J. M., Chanenson, S. L., & Bergstrom, M. H. (2011). Reform in Motion: The Promise and Perils of Incorporating Risk Assessments and Cost-Benefit Analysis into Pennsylvania Sentencing The Sentencing Issue: Sentencing in the Federal Arena and in Pennsylvania. *Duquesne Law Review*, 49(4), 707–750.
- Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1), 1–6. <https://doi.org/10.5281/zenodo.18276>
- Jasanoff, S. (2015). Future imperfect: Science, technology, and the imaginations of modernity. In S. Jasanoff & S.H. Kim (Eds.), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (pp. 1-33). Chicago: University of Chicago Press.
- Jefferson, B. (2020). *Digitize and Punish: Racial Criminalization in the Digital Age*. University of Minnesota Press. <https://doi.org/10.5749/j.ctvz0h9s7>
- Jewitt, C., Price, S., Leder Mackley, K., Yiannoutsou, N., & Atkinson, D. (2020). *Interdisciplinary Insights for Digital Touch Communication*. Springer Nature. <https://doi.org/10.1007/978-3-030-24564-1>
- Jewkes, Y., & Reisdorf, B. C. (2016). A brave new world: The problems and opportunities presented by new media technologies in prisons. *Criminology & Criminal Justice*, 16(5), 534–551. <https://doi.org/10.1177/1748895816654953>
- Joh, E. E. (2014). Policing by Numbers: Big Data and the Fourth Amendment Essay. *Washington Law Review*, 89(1), 35–68.
- Joh, E. E. (2016). The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing Symposium: Policing in America on the 50th Anniversary of *Miranda v. Arizona*. *Harvard Law & Policy Review*, 10(1), 15–42.
- Jones, R. (2000). Digital Rule: Punishment, Control and Technology. *Punishment & Society*, 2(1), 5–22. <https://doi.org/10.1177/14624740022227836>
- Kaun, A., & Stiernstedt, F. (2020). Doing time, the smart way? Temporalities of the smart prison. *New Media & Society*, 22(9), 1580–1599. <https://doi.org/10.1177/1461444820914865>
- Kehl, D., Guo, P., & Kessler, S. (2017). *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*. <https://dash.harvard.edu/handle/1/33746041>
- Lageson, S. (2020). *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. Oxford University Press.
- Lageson, S. E. (2022). Criminal Record Stigma and Surveillance in the Digital Age. *Annual Review of Criminology*, 5(1), 67–90. <https://doi.org/10.1146/annurev-criminol-030920-092833>

- Lavorgna, A., & Ugwudike, P. (2021). The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control. *Big Data & Society*, 8(2), 20539517211049670. <https://doi.org/10.1177/20539517211049670>
- Lazer, D., & Radford, J. (2017). Data ex Machina: Introduction to Big Data. *Annual Review of Sociology*, 43(1), 19–39. <https://doi.org/10.1146/annurev-soc-060116-053457>
- Liu, H.-W., Lin, C.-F., & Chen, Y.-J. (2019). Beyond State v Loomis: Artificial intelligence, government algorithmization and accountability. *International Journal of Law and Information Technology*, 27(2), 122–141. <https://doi.org/10.1093/ijlit/eaz001>
- Livingston, J. (2021). Artificial Intelligence and Public Law. In M. Valverde, K. Clarke, E. Darian-Smith & P. Kotiswaran (Eds.), *The Routledge Handbook of Law and Society* (pp. 76-80). Routledge.
- Lupton, D. (2015). *Digital sociology*. Routledge, Taylor & Francis Group.
- Lynch, M. (1998). Waste Managers? The New Penology, Crime Fighting, and Parole Agent Identity. *Law & Society Review*, 32(4), 839–869. <https://doi.org/10.2307/827741>
- Lynch, M. (2019). The Narrative of the Number: Quantification in Criminal Court. *Law & Social Inquiry*, 44(1), 31–57. <https://doi.org/10.1111/lsi.12334>
- Mahoney, J. (2000). Strategies of causal inference in small-N analysis. *Sociological methods & research*, 28(4), 387-424.
- Massaro, V. A., Dhar, S., Mir, D., & Ryan, N. C. (2022). Carceral algorithms and the history of control: An analysis of the Pennsylvania additive classification tool. *Big Data & Society*, 9(1), 20539517221094000. <https://doi.org/10.1177/20539517221094002>
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution that Will Transform how We Live, Work, and Think*. Houghton Mifflin Harcourt.
- McDaniel, J. L. M., & Pease, K. (2021). *Predictive Policing and Artificial Intelligence*. Routledge. <https://doi.org/10.4324/9780429265365>
- Mehozay, Y., & Fisher, E. (2019). The epistemology of algorithmic risk assessment and the path towards a non-penology penology. *Punishment & Society*, 21(5), 523–541. <https://doi.org/10.1177/1462474518802336>
- Miller, L. L. (2001). Looking for Postmodernism in All the Wrong Places: Implementing a New Penology. *British Journal of Criminology*, 41(1), 168–184.
- Mufarreh, A., Waitkus, J., & Booker, T. A. (2021). Prison official perceptions of technology in prison. *Punishment & Society*, 1462474521990777. <https://doi.org/10.1177/1462474521990777>
- Nair, V. (2021). Becoming data: Biometric IDs and the individual in ‘Digital India.’ *Journal of the Royal Anthropological Institute*, 27(S1), 26–42. <https://doi.org/10.1111/1467-9655.13478>
- O’Malley, P. (1992). Risk, power and crime prevention. *Economy and Society*, 21(3), 252–275. <https://doi.org/10.1080/03085149200000013>
- Plesničar, M. M., & Stubbs, K. Š. (2017). Subjectivity, algorithms and the courtroom. In *Big Data, Crime and Social Control*. Routledge.
- Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology: Crime and Justice in Digital Society*. Routledge. <https://doi.org/10.4324/9781315205786>
- Rapaport, W. J. (2012). Semiotic Systems, Computers, and the Mind: How Cognition Could Be Computing. *International Journal of Signs and Semiotic Systems (IJSSS)*, 2(1), 32–71. <https://doi.org/10.4018/ijsss.2012010102>

- Rice, R., Yates, S., & Blejmar, J. (2020). Introduction to the Oxford Handbook of Digital Technology and Society: Terms, Domains, and Themes. In S. Yates & R. Rice (Eds.), *The Oxford Handbook of Digital Technology and Society* (pp. 4–35). Oxford University Press.
- Ridgeway, G. (2018). Policing in the Era of Big Data. *Annual Review of Criminology*, 1(1), 401–419. <https://doi.org/10.1146/annurev-criminol-062217-114209>
- Rubin, A. T. (2016). Penal change as penal layering: A case study of proto-prison adoption and capital punishment reduction, 1785–1822. *Punishment & Society*, 18(4), 420–441. <https://doi.org/10.1177/1462474516641376>
- Rubin, A. T. (2021). The promises and pitfalls of path dependence frameworks for analyzing penal change. *Punishment & Society*, 14624745211043544. <https://doi.org/10.1177/14624745211043544>
- Russell, S. J., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (Third edition.). Prentice Hall.
- Seeds, C. (2022). *Death by Prison: The Emergence of Life without Parole and Perpetual Confinement*. University of California Press.
- Selbst, A. D. (2017). Disparate Impact in Big Data Policing. *Georgia Law Review*, 52(1), 109–196.
- Simon, J. (1988). The Ideological Effects of Actuarial Practices. *Law & Society Review*, 22(4), 771–800.
- Simon, J. (2013). Punishment and the political technologies of the body. *The SAGE Handbook of Punishment and Society*, 60–89.
- Smith, G., Bennett Moses, L., & Chan, J. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*, 57(2), 259–274. <https://doi.org/10.1093/bjc/azw096>
- Smith, P. (2003). Narrating the Guillotine: Punishment Technology as Myth and Symbol. *Theory, Culture & Society*, 20(5), 27–51. <https://doi.org/10.1177/02632764030205002>
- Sourdin, T., Meredith, J., & Li, B. (2020). *Digital Technology and Justice: Justice Apps*. Routledge.
- Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a ‘Digital Criminology’? *International Journal for Crime, Justice and Social Democracy*, 6(2), 17–33. <http://dx.doi.org/10.5204/ijcjsd.v6i2.355>
- Ugwudike, P. (2020). Digital prediction technologies in the justice system: The implications of a ‘race-neutral’ agenda. *Theoretical Criminology*, 24(3), 482–501. <https://doi.org/10.1177/1362480619896006>
- Willis, J. (2005). Transportation versus Imprisonment in Eighteenth and Nineteenth Century Britain: Penal Power, Liberty, and the State. *Law & Society Review* 39(1): 171-210.
- Završnik, A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*, 18(5), 623–642. <https://doi.org/10.1177/1477370819876762>