RUMO A UMA IMPLEMENTAÇÃO TRANSPARENTE, ÉTICA E INCLUSIVA DAS TECNOLOGIAS – O CASO DE *BIG DATA* NA PREVISÃO CRIMINAL

TOWARDS A TRANSPARENT, ETHICAL, AND INCLUSIVE IMPLEMENTATION OF TECHNOLOGIES — THE CASE OF *BIG DATA* IN CRIME PREDICTION

LAURA NEIVA[1]

HELENA MACHADO[2]

Resumo

Este texto reflete sobre a utilização de *Big Data* na previsão criminal e o seu potencial para desencadear efeitos de desempoderamento, entendidos como consequências sociais negativas sobre indivíduos, grupos e sociedades. Considerando as linhas orientadoras da inovação responsável, argumentamos sobre a necessidade de promover um debate interdisciplinar e colaborativo sobre a implementação de *Big Data* na previsão criminal, alicerçado na deliberação de três valores – robustez, utilidade e legitimidade. Um exercício participativo desta natureza, orientado para o envolvimento público nas deliberações sobre os usos legítimos de tecnologias, permite reforçar princípios de responsabilização e transparência, inclusão e igualdade social. Como tal, configura-se um instrumento crucial para a confiança pública na tecnologia e para a democracia.

1 Departamento de Sociologia, Doutoramento em Sociologia, Centro de Estudos de Comunicação e Sociedade, Instituto de Ciências Sociais, Universidade do Minho. E-mail: lauraneiva@ics.uminho.pt, ORCID: 0000-0002-1954-7597.

2 Departamento de Sociologia, Instituto de Ciências Sociais, Universidade do Minho. E-mail: hmachado@ics.uminho.pt, ORCID: 0000-0001-8554-7619.

Palavras-chave: *Big Data*; previsão criminal; inovação responsável; envolvimento público; tecnologia.

Abstract
This text reflects on the use of *Big Data* in criminal prediction and its potential to trigger disempowerment effects, understood as negative social consequences on individuals, groups and societies. Considering the guidelines for responsible innovation, we emphasize the need to promote an interdisciplinary and collaborative debate on the implementation of *Big Data* in criminal prediction, based on the deliberation of three values – robustness, usefulness and legitimacy. A participatory exercise of this nature, oriented towards public involvement in deliberations on the legitimate uses of technologies, makes it possible to reinforce principles of accountability and transparency, inclusion and social equality. Therefore, it might be a crucial instrument for public trust in technology, and for democracy.
Keywords: *Big Data*; crime prediction; responsible innovation; public engagement; technology.

1. Introdução

A expansão do uso de tecnologias de *Big Data*[3] para fins de policiamento e de segurança é marcante nos últimos anos dadas as suas capacidades técnicas em produzir informações sobre eventos criminais, a partir do acesso, processamento e análise de conjuntos massivos de dados provenientes de diversas fontes. Os discursos otimistas enfatizam o poder das tecnologias de *Big Data* para potenciar a celeridade e eficiência do sistema de justiça criminal por via das suas esperadas valências na previsão e eventual redução da criminalidade (Marciani *et al.*, 2017; Plaksiy *et al.*, 2018; Pramanik *et al.*, 2017). O risco da disseminação destes discursos laudatórios sobre *Big Data* é que, repletos de entusiasmo em torno do poder da tecnologia, restringem as reflexões em torno dos seus limites, viés e consequências sociais negativas. Dados os erros que lhe são inerentes, com impactos na exacerbação das velhas desigualdades sociais e práticas desproporcionais do sistema de justiça criminal[4] (Berk, 2021; Minocher & Randall, 2020; Završnik, 2019), a sua aplicação tem desencadeado o que Van Brakel (2016, p. 123) designa por "efeitos de desempoderamento de *Big Data*" para se referir ao

3 Adotando a lente dos Estudos Sociais da Ciência e Tecnologia, o presente texto concebe *Big Data* como uma tecnologia: um sistema socialmente construído, imbuído de valores humanos, lógicas, crenças e visões culturais, sociais e políticas (Aradau & Blanke, 2015; Bijker & Law, 1992; Chan & Moses, 2017).

4 Como a suspeição criminal e marginalização histórica de grupos vulneráveis do ponto de vista socioeconómico e minorias étnicas.

"conjunto de consequências sociais negativas provocadas pela aplicação de *Big Data*, com impactos nos indivíduos, grupos e sociedades"[5].

Considerando estes "efeitos de desempoderamento de *Big Data*", que fragilizam a responsabilização e transparência, a inclusão e igualdade social, e a confiança e democracia, o presente texto reflete sobre modalidades possíveis de "governação antecipatória"[6] (Guston, 2014, p. 219). Esta é entendida como a possibilidade de envolver uma parte significativa da sociedade na governabilidade de tecnologias emergentes, antecipando os seus riscos e consequências, por via do cruzamento de perspetivas plurais e diversificadas. No caso que nos ocupa no presente texto, trata-se de promover a compreensão alargada dos desafios e impactos presentes e futuros que as tecnologias de *Big Data* apresentam(rão), de modo a antecipá-los por via de debates que incluam vários atores sociais, envolvendo-os na deliberação sobre modos de implementação de *Big Data* na previsão criminal.

Em termos práticos, partindo de um conjunto de estratégias assentes na ponderação de três valores – robustez, utilidade e legitimidade[7] (R.U.LE.) –, proposto por Wienroth (2020, p. 1), pretende-se desenvolver práticas que visem contribuir para que a aplicação da tecnologia de *Big Data* no contexto da previsão criminal seja informada pelas visões do público e de outros *stakeholders*[8]. Através do envolvimento de diversos atores sociais, desde legisladores, a órgãos governamentais, cidadãos e organizações da sociedade civil, o conjunto de estratégias que apresentamos trilha novos caminhos rumo a uma implementação ética, transparente e inclusiva de *Big Data* para fins de previsão criminal. Assim, encorajamos a consciencialização dos diferentes atores sociais sobre a sua posição, papel e responsabilidades na aplicação desta tecnologia, propondo que, através de um debate colaborativo e interdisciplinar, se reflita sobre as esperanças, preocupações e ansiedades em torno de *Big Data* neste contexto.

O texto encontra-se estruturado em quatro partes. Num primeiro momento apresentamos a concetualização de *Big Data* na previsão criminal, com exemplos práticos da sua aplicação, enfatizando os erros que lhe são inerentes. De seguida, exploramos os "efeitos de desempoderamento de *Big Data*" como consequências sociais negativas sobre indivíduos, grupos e sociedades. Na secção seguinte, apresentamos um conjunto de estratégias assentes na deliberação de valores como a robustez, utilidade e legitimidade. Por fim, a conclusão sistematiza as principais características

5 Todos os excertos incluídos no texto foram traduzidos de inglês para português. Esta tradução é da total responsabilidade das autoras.

6 Tradução portuguesa do conceito *antecipatory governance.*

7 Tradução portuguesa dos conceitos *reliability*, *utility* and *legitimacy*.

8 Consideramos a definição de Micheli *et al.* (2020, p. 5) de stakeholders como "indivíduos, instituições, organizações ou grupos que são afetados, ou têm efeito no modo como os dados são governados e no valor que lhes é conferido".

de um exercício participativo desta natureza, orientado para o envolvimento público nas deliberações sobre os usos legítimos de tecnologias, permitindo reforçar princípios de responsabilização e transparência, inclusão e igualdade social.

Como tal, este exercício participativo configura-se um instrumento crucial para a confiança pública na tecnologia e para a democracia.

2. *Big Data* e previsão criminal

As tecnologias de *Big Data* aplicadas no campo securitário com objetivos de previsão criminal visam cumprir finalidades de governação antecipatória para o crime (Aradau, 2015; Aradau & Blanke, 2017; Van Brakel & De Hert, 2011). A sua aplicação para fins de previsão criminal almeja cumprir três objetivos (Perry *et al.*, 2013): i) a previsão de perpetradores, por exemplo, por via da antecipação da reincidência criminal, ou seja, pela identificação de indivíduos que poderão potencialmente cometer crimes no futuro, com base em análises dos seus antecedentes criminais e características (Berk *et al.*, 2009); ii) previsão de vítimas, ou seja, de pessoas que apresentam maior probabilidade de serem alvo de um crime, com base em dados de vítimas conhecidas (Ratcliffe, 2014); e iii) previsão do local e intervalo temporal onde é mais provável de um crime ocorrer (Hardyns & Rummens, 2018; Meijer & Wessels, 2019; Perry *et al.*, 2013; Sandhu & Fussey, 2021). Considerando o propósito do presente texto, referimo-nos a tecnologias de *Big Data* para fins de previsão criminal que cumpram o primeiro e último objetivo.

De um modo geral, as tecnologias de *Big Data* para fins de previsão criminal caracterizam-se pela recolha sistemática e orientada de dados para posterior cruzamento e processamento, cujo objetivo é o de criar perfis criminais que auxiliem a atuação policial antes que as ameaças se concretizem (Lyon, 2014, p. 2; Van Brakel, 2016). Em termos práticos, materializam-se através de sistemas de algoritmos aptos para pesquisar, classificar, armazenar e combinar dados (não) estruturados, comparando-os entre si e com outros dados. Deste modo, criam correspondências posteriormente inseridas em sistemas de inteligência artificial, que permitem encontrar padrões e criar conhecimento estratégico operacional, com o objetivo de prever o crime e/ou os seus autores (Van Brakel, 2021, p. 233). No entanto, vários estudos têm indicado que a eficácia destas estratégias é questionável na medida em que não está provada a sua eficiência em termos de efeitos operacionais na previsão criminal, e, além disso, têm sido detetados erros nos *softwares* (Berk, 2021; Egbert, 2019; Hardyns & Rummens, 2018; Meijer & Wessels, 2019). Ademais, quando estas estratégias de previsão criminal são comparadas com outras intervenções tradicionais policiais, como o patrulhamento pedestre, não são aferidas mudanças na redução das taxas de criminalidade, não produzindo os efeitos práticos esperados (Browning & Arrigo, 2021).

Hardyns e Rummens (2018, p. 207), na descrição que apresentam sobre os três *softwares* de previsão criminal mais aplicados nos Departamentos Policiais na

Europa – o *Crime Anticipation System* (CAS), o *PreCobs* e o *PredPol* –, enfatizam os erros e o viés que lhes são inerentes. O CAS foi desenvolvido para prever crimes como assaltos, furtos e outros crimes violentos, a partir de dados históricos, sociodemográficos, económicos e geográficos de áreas sinalizadas com alto risco criminal pela polícia. No entanto, dado o grande volume de dados que analisa, as suas análises não têm produzido qualquer tipo de relação com a criminalidade. Por sua vez, o *PreCobs* foi desenvolvido para prever assaltos a residências, a partir de informações histórico-temporais, espaciais e de *modus operandi* na perpetuação deste tipo de crime. No entanto, até ao momento, não existe informação que ateste a sua eficácia (Hardyns & Rummens, 2018). Por fim, o *PredPol* foi criado para sofisticar as análises preditivas no tempo e no espaço. Baseado em dados criminais passados, calcula previsões sobre tipos de crime, locais de ocorrência e intervalos de tempo, delineando mapas de frequência criminal. No entanto, dado que a criminalidade varia no tempo, espaço e natureza, os resultados produzidos têm sido bastante falaciosos (Aradau & Blanke, 2017; Hardyns & Rummens, 2018).

Não obstante, tem havido procura crescente destes *softwares* dado que vários países estão a investir em novas tecnologias de previsão criminal (Jackson *et al.*, 2014; Nationale Politie, 2015; College of Policing, 2016). Esta expansão de *Big Data* tem desencadeado consequências associadas a "efeitos de desempoderamento" (Van Brakel, 2016, p. 123), conforme detalhamos de seguida.

3. "Efeitos de desempoderamento de *Big Data*" e os seus impactos

Os "efeitos de desempoderamento de *Big Data*" (Van Brakel, 2016, p. 123), significam o "conjunto de consequências sociais negativas provocados pela aplicação de *Big Data*, com impactos nos indivíduos, grupos e sociedades", com potencial para refletir velhas desigualdades sociais e práticas desproporcionais do sistema de justiça criminal. Por exemplo, a suspeição criminal e marginalização histórica de grupos vulneráveis do ponto de vista socioeconómico e minorias étnicas, com implicações ao nível da inclusão e igualdade social, como exploraremos.

A tabela 1 apresenta uma sistematização dos "efeitos de desempoderamento de *Big Data*".

Tabela 1. *Big Data* na previsão criminal: desempoderamento e ações necessárias

Efeitos de desempoderamento	Ações necessárias
- Tomada de decisões com base em algoritmos - Procedimentos técnicos obscuros (opacidade)	Responsabilização e transparência

- Sobrerrepresentação de grupos sociais minoritários nas bases de dados policiais	Inclusão e igualdade social
- Implementação da tecnologia sem envolvimento público	Confiança e democracia

Fonte: Autoras (inspiradas em Van Brakel, 2016, 2021).

Nas secções que se seguem, apresentamos, de modo detalhado, de que forma os efeitos de desempoderamento gerados pelos usos de *Big Data* na previsão criminal podem ser mitigados por via de ações assentes na responsabilização e transparência; inclusão e igualdade social; e confiança e democracia.

3.1. Algoritmos e opacidade versus responsabilização e transparência

A crescente tendência para a implementação de tecnologias de *Big Data*, aptas a calcular algoritmos a partir de informações criminais passadas, visa nortear previsões criminais, movendo a responsabilização humana das decisões. Isto significa que, considerando que a tecnologia produz dados que informam a previsão criminal, os algoritmos que calcula serão determinantes no momento de uma intervenção policial, sendo estes *softwares* responsáveis pela tomada de decisão. Consequentemente, também os erros e o viés dos resultados produzidos pelos sistemas de *Big Data* são atribuídos à própria tecnologia pelos seus manuseadores (neste caso, agentes policiais ou outros profissionais do sistema de justiça criminal, por exemplo) (Van Brakel, 2016). Embora no policiamento os resultados produzidos de modo automático pela tecnologia careçam de uma validação humana (Andrejevic *et al.*, 2020; Chan & Moses, 2017; Dencik *et al.*, 2018; Egbert & Krasmann, 2020; Kaufmann *et al.*, 2019; Sanders *et al.*, 2015; Sandhu & Fussey, 2021), tal como Van Brakel (2016, p. 124) refere "não é improvável que as futuras decisões sobre intervenções sejam cada vez mais feitas pela tecnologia". Face a potenciais erros e viés, diz o autor, "não fica claro quem é responsabilizado: a empresa que desenvolveu a tecnologia, o cientista que delineou o algoritmo ou o legislador que autorizou a sua implementação?" (Van Brakel, 2016, p. 124).

A título de exemplo, Larson e colegas (2016) analisaram o modo como operava o COMPAS, um *software* desenvolvido para prever a reincidência de reclusos e utilizado nos Estados Unidos da América como fator preponderante no momento da decisão de conferir liberdade condicional. Os autores concluíram que indivíduos de raça negra tinham, em todos os casos, maior probabilidade de serem categorizados com alto risco de reincidência, quando comparados com indivíduos caucasianos. No entanto, na maior parte dos casos observados, nos anos seguintes, os indivíduos de raça negra não reincidiam, contrariamente ao que fora previsto pela tecnologia. Nestas situações, a decisão de não conceder liberdade condicional a estes indivíduos

por terem sido classificados de "alto risco" no *software* determina o cumprimento total da pena (Larson *et al.*, 2016). Tal como Lyon (2007, p. 186) refere, "quando as oportunidades de vida de um indivíduo dependem da categoria onde este foi colocado, é muito importante saber quem desenhou as categorias, quem define o seu valor e quem decide em que circunstâncias essas categorias serão decisivas". Dada a inadequação do atual enquadramento legislativo para a tecnologia de *Big Data* na previsão criminal, que não apresenta respostas claras a estas questões (Neiva & Machado, 2021), Van Brakel e De Hert (2011) alertam para o facto de ser tentador responsabilizar o sistema tecnológico, dada a inexistência de *standards* legais e políticos que permitam enquadrar e definir as ações e agentes englobáveis em processos institucionais, formalmente definidos, de responsabilização.

Observa-se também que os procedimentos através dos quais os dados são inseridos nos *softwares* e o modo como o algoritmo cria categorias não são claros, dado que os produtores deste tipo de tecnologias raramente partilham o modo como foram criadas e os procedimentos através dos quais os dados são acedidos e armazenados (Leese, 2014). Isso dificulta a intervenção em cada etapa do processamento automatizado e a minimização das margens de erro. A (re)produção de erros deriva da forma como os dados são obtidos e tratados automaticamente, afetando a transparência dos procedimentos técnicos das tecnologias (Van Brakel, 2016). Por exemplo, os dados usados pelo *PredPol* para calcular algoritmos de previsão criminal são inseridos pela empresa responsável pelo seu desenvolvimento. Outros *softwares* de previsão criminal também não são claros relativamente ao modo como os perfis "suspeitos" são criados, como se desenvolvem ameaças, ou como o algoritmo é programado. Uma parte considerável desta falta de transparência reside na origem do *software* – da empresa que o programou – e, também, nos próprios dados incluídos no programa informático (Van Brakel, 2016).

3.2. Discriminação versus inclusão e igualdade social

Fruto da falta de transparência e responsabilização, os impactos estendem-se aos efeitos sociais da aplicação das tecnologias de *Big Data* e amplamente discutidos noutros estudos, como a perpetuação da racialização e discriminação, estigmatização algorítmica e expansão das desigualdades sociais (Benbouzid, 2019; Berk, 2021; Ferguson, 2015; Joh, 2014, 2016; Kaufmann *et al.*, 2019; Lei, 2019; Minocher & Randall, 2020; Neiva, 2020).

As categorias produzidas nestes *softwares* de previsão criminal são traduzidas em códigos computacionais e esta tradução pode produzir consequências, dado que a categorização dos dados pode gerar erros (Kitchin, 2014) que podem conduzir a acusações falsas (Ferguson, 2015). Uma taxa alta de falsos positivos aumenta a probabilidade de certos indivíduos e grupos serem sistemática e desproporcionalmente classificados como potenciais criminosos (Van Brakel, 2016).

Ademais, a grande maioria dos *softwares* preditivos baseia-se em dados criminais passados[9] sobre os quais se baseia a previsão criminal futura. Na prática, contribui para que estas previsões incidam sempre sobre os mesmos suspeitos, reproduzindo as ações discricionárias dos agentes policiais e dos sistemas de justiça. Além de (re)produzir desigualdades sociais, exacerba a estigmatização e criminalização das comunidades mais vulneráveis à suspeição criminal (Brayne, 2017; Johnson & Rostain, 2020; Lyon, 2014; Matzner, 2016), categorizando-as como alvos e colocando-as sob escopo do sistema de justiça criminal (Benbouzid, 2019; Berk, 2021; Brayne, 2017; Browning & Arrigo, 2021; Lyon, 2014; Matzner, 2016; Sandhu & Fussey, 2021). Deste modo, estes *softwares* contribuem para exacerbar diferenças entre grupos sociais a partir de variáveis como a classe social, a etnia e raça, a área de residência e o histórico criminal (Neiva, 2021). Consequentemente, o modo como classificam as populações, afeta as oportunidades de vida dos cidadãos (Monahan, 2010), contribuindo para o reforço da exclusão social de grupos já socialmente vulneráveis e marginalizados, nomeadamente, migrantes, minorias étnicas e indivíduos em situação de pobreza (Brayne, 2014).

3.3. Falta de envolvimento público versus confiança e democracia

As tecnologias de *Big Data*, à semelhança de outras tecnologias na investigação criminal como, por exemplo, a tecnologia de inferência fenotípica, que permite 'prever' a aparência física e 'raça' de uma pessoa (ver Wienroth, 2020) são desenvolvidas sem que se verifique uma deliberação interdisciplinar que pudesse auxiliar no delineamento do seu *design* e posterior implementação. Nos últimos anos, assistimos a vários pedidos de pareceres à Comissão Nacional de Proteção de Dados, enquanto entidade independente com poderes de autoridade para controlo e fiscalização de processamentos de dados pessoais, para avaliação da legitimidade de aplicação de tecnologias para fins de segurança[10]. No entanto, este tipo de pedidos a órgãos independentes acontecem geralmente *a posteriori*, ou seja: o desenvolvimento e utilização de uma tecnologia é mais precoce e acelerado que o ritmo de governação legal e eticamente responsáveis.

Em primeiro lugar, as empresas que desenvolvem este tipo de tecnologias raramente partilham o modo como foram criadas, nem veiculam publicamente os procedimentos através dos quais os dados são acedidos e armazenados. Neste contexto, são sérias as limitações à compreensão dos erros e mapeamento de viés inerentes à utilização de uma dada tecnologia. Esta postura generalizada de fechamento e opacidade dificulta o desenvolvimento de procedimentos que possam minimizar as margens de erros das tecnologias que seriam viáveis caso fossem conhecidos os seus modos de produção de resultados estatísticos. Consequentemente, este tipo de práticas

9 Como explanado na secção *2. Big Data e previsão criminal* deste texto.

10 Como aconteceu, por exemplo, no âmbito da instalação de circuitos de videovigilância em Portugal (Machado & Frois, 2014, p. 71).

acentua a reprodução de conclusões inválidas ou erróneas (Leese, 2014), defraudando a confiança pública nas tecnologias. Por sua vez, embora estes processos sejam opacos perante a sociedade, os discursos políticos tendem a promover a confiança em torno destas tecnologias (Neiva & Machado, 2021), sem o desejável envolvimento do público, de profissionais e de outros *stakeholders* na compreensão dos procedimentos de recolha, análise e processamento dos dados (Aradau, 2015).

Estas práticas comumente generalizadas de ausência de participação ou representação pública em processos deliberativos em torno de tecnologias emergentes que afetam diversos públicos – sobretudo os indivíduos, grupos e comunidades em maior risco de caírem nas malhas da suspeição de agentes policiais e do sistema de justiça criminal – nas palavras de Monahan (2010, p. 91) "são claramente não democráticas". Na ausência de um debate interdisciplinar e coletivo, fica limitada a antecipação das consequências negativas (e, até, imprevisíveis), fenómeno esse que poderia ser minimizado se o *design* da tecnologia em questão e a sua implementação abarcasse visões de vários públicos (Guston, 2014; Wienroth, 2020).

4. Estratégias para uma implementação transparente, ética e inclusiva de *Big Data* na previsão criminal

Sugerimos uma abordagem que, baseada num conjunto de propostas de implementação concreta, possa promover um diálogo interdisciplinar para a implementação desta tecnologia no campo da previsão criminal. Apresentamos uma proposta de um conjunto de práticas assentes na deliberação de três valores – robustez, utilidade e legitimidade que nortearão uma implementação transparente, ética e inclusiva de *Big Data* neste campo, com potencial para antecipar e minimizar os "efeitos de desempoderamento de *Big Data*" (Van Brakel, 2016). Este conjunto de práticas privilegia o envolvimento ativo da sociedade, dos cidadãos, de empresas privadas, órgãos governamentais e demais *stakeholders* na definição do modo como a tecnologia deve ser implementada nos contextos de promoção securitária (Van Brakel, 2016). A partir do conhecimento de todos os envolvidos, visa-se contribuir para uma "governação antecipatória" das tecnologias, promovida através de *focus group*[11] ou conferências de consenso[12] (Guston, 2014). Nestas sessões de debate, diferentes atores sociais são encorajados a partilhar as suas experiências, esperanças e expectativas acerca da implementação de *Big Data* na previsão criminal. A inclusão de diferentes públicos é importante dado que, à semelhança do que Guston (2014, p. 229) refletiu sobre práticas de governança antecipatória a propósito da nanotecnologia, a tecnologia é compreendida de modo

11 Discussão estruturada de um grupo de pessoas, dirigida por um moderador, que visa incitar a reflexão e debate sobre um tema específico, por via da colocação de um conjunto de questões abertas (Masadeh, 2012).

12 Envolvem grupos de pessoas com conhecimentos sobre uma determinada questão e desenvolvem uma avaliação de questões-chave identificadas como críticas sobre o tema (Einsiedel & Eastlick, 2000).

distinto pelos diferentes atores sociais. Este tipo de iniciativas potenciará o desenvolvimento de um futuro técnico para *Big Data* informado pela ética e transparência, antecipando os seus impactos. A tabela 2 sistematiza, em termos práticos, as estratégias que desenvolvemos.

Tabela 2. Conjunto de estratégias assentes em valores de robustez, utilidade e legitimidade

Valores	Conjunto de estratégias		
	Questões-chave	**Como deliberar?**	**Quem envolver?**
Robustez	A tecnologia é confiável do ponto de vista técnico e científico?	Debater erros e viés da tecnologia *vs* robustez dos dados	• Polícias • Legisladores • Cidadãos • Organizações não governamentais • Empresas responsáveis pelo desenvolvimento destas tecnologias • Profissionais do sistema de justiça criminal • Outros *stakeholders*
Utilidade	A tecnologia é vantajosa?	Explorar (des)vantagens do seu uso	
Legitimidade	Como utilizar a tecnologia de modo responsável?	Analisar os custos morais de *Big Data*	

Fonte: Autoras (inspiradas em Van Brakel, 2016 e Wienroth, 2020).

4.1 Robustez

A robustez relaciona-se com a validade da tecnologia, ou seja, o modo como esta se operacionaliza e que dados utiliza para alcançar resultados fiáveis e confiáveis (Wienroth, 2020). A validade dos dados diz respeito ao modo como as informações são produzidas nas pesquisas e análises que são realizadas pela tecnologia de *Big Data*. Esta deve ser deliberada através de debates em torno dos erros e viés de *Big Data*, bem como, sobre a qualidade dos dados sob os quais os algoritmos de *Big Data* realizam as análises e produzem resultados de previsão criminal. Isto significa explorar, de modo transparente, os viés inerentes à tecnologia e aos dados que a informam. Os "efeitos de desempoderamento" abordados anteriormente como preconceito racial e discriminação de certos grupos sociais reproduzidos nos resultados obtidos pelo *Big Data* são reflexo de uma sobrerrepresentação de informações sobre determinadas camadas sociais nas bases de dados policiais. Se os algoritmos de *Big Data* são informados por essas informações enviesadas, produzirão resultados de previsão criminal sobre os dados que contêm erros, conduzindo a intervenções desproporcionais e desiguais do sistema de justiça criminal que afetam claramente

grupos sociais desapossados (Benbouzid, 2019; Berk, 2021; Brayne, 2017; Browning & Arrigo, 2021; Lyon, 2014; Matzner, 2016; Sandhu & Fussey, 2021).

Um debate que promova a deliberação e o entendimento sobre estes erros permitirá compreender a qualidade dos dados utilizados para informar a previsão criminal, o que consequentemente, requererá transparência sobre o contexto que conduzirá e possibilitará a implementação de *Big Data*. Significará debater, através da inclusão participativa de diferentes atores sociais, os contextos organizacionais onde a tecnologia se desenvolverá e será aplicada, de modo a descortinar os seus erros, antecipando-os e desenvolvendo estratégias que os possam minimizar. Uma aproximação a estes contextos e práticas permitirá explorar a origem e qualidade das informações inseridas nas bases de dados de forma a compreender os seus erros e viés (Wienroth, 2020). Por exemplo, no cálculo de correlações probabilísticas erradas, que podem conduzir a acusações criminais falsas, equacionando modos de os mitigar. Para tal, é necessário consciencializar os atores sociais sobre os impactos negativos do *Big Data*, (re)centrando o foco do debate para os efeitos de desempoderamento desta tecnologia (Van Brakel, 2016). Assim, sugerimos um debate público acerca dos erros da tecnologia, instigando a questões práticas como: Como funciona a tecnologia? Quais são os erros de *Big Data*? Estão os profissionais conscientes destes erros? E como podem ser mitigados?

Finalmente, ao consciencializar deste modo os manuseadores de tecnologias de *Big Data*, desenvolvemos o seu entendimento sobre as margens de erro da tecnologia, os seus limites e modos operacionais de os gerir. Para tal, também é necessário atingir um consenso sobre: que tipo de *software* de *Big Data* utilizar? Como os dados/resultados obtidos devem ser interpretados? Estes dados podem ser partilhados? Debatendo a robustez das tecnologias e promovendo a confiança na divulgação e utilização dos resultados produzidos pela tecnologia (Wienroth, 2020), potenciar-se-á o entendimento do papel das decisões tomadas e da posição profissional de cada ator social no processo de inovação, delineando um desenvolvimento responsável da tecnologia (Guston, 2014).

4.2 Utilidade

As considerações sobre a utilidade relacionam-se com a robustez, pois uma tecnologia é considerada útil se possuir valor operacional e for fiável do ponto de vista técnico e científico (Wienroth, 2020). Por exemplo, se a tecnologia de *Big Data* produz dados que auxiliam a previsão criminal, será considerada útil e eficaz. No entanto, tal como Wienroth (2020, pp. 6-7) refere, a utilidade das tecnologias está ligada à ordem pública e social pois a sua utilização no sistema de justiça criminal tem como finalidade o restabelecimento destas após um crime ocorrer. Possíveis desrespeitos a liberdades civis e outros direitos humanos devido ao uso da tecnologia podem provocar efeitos adversos se forem percecionados como consequências de um uso inapropriado da tecnologia. Utilizar tecnologias de *Big Data* para prever quando, onde e quem cometerá o próximo

crime e partilhar essas probabilidades, pode alimentar preconceitos, incitando ações de exclusão contra grupos minoritários, por exemplo. Assim, sugerimos uma deliberação interdisciplinar em torno das vantagens e desvantagens do uso de *Big Data* para fins de previsão criminal, capaz de, ao ser informada por visões e conhecimentos diversos, debater os aspetos positivos e negativos da sua utilização.

Em termos práticos, propomos um debate que considere duas hipóteses centrais: (i) os algoritmos de *Big Data* produzem dados e informações para nortear atividades de previsão criminal; (ii) no entanto, a sua utilização pode desencadear efeitos negativos, tais como acusações criminais falsas, desproporcionais e preconceituosas, além da sua eficácia prática não ter sido ainda comprovada (Berk, 2021; Egbert, 2019; Hardyns & Rummens, 2018; Meijer & Wessels, 2019). Como equilibrar as suas vantagens e desvantagens? É importante considerar os seus riscos e benefícios, seguindo os princípios da Pesquisa e Inovação Responsáveis[13] (RRI) e antecipando e avaliando as potenciais implicações sociais da inovação (Betten *et al.*, 2018; Yu, 2016).

4.3 Legitimidade

Por fim, uma deliberação interdisciplinar das tecnologias é crucial para explorar a legitimidade de *Big Data*. Esta deve ser analisada por via da relação entre a implementação de tecnologias de *Big Data* e os seus custos éticos, morais, sociais e legais. A legitimidade invoca reflexões em torno da robustez moral de *Big Data* na previsão criminal e do modo como esta tecnologia pode ser utilizada de forma responsável. Para tal, propomos que se discutam aspetos em torno do seu contexto legislativo e regulatório, atendendo aos discursos e debates políticos sobre a sua implementação no contexto de aplicação da lei (Wienroth, 2020).

Por exemplo, analisando: (i) os motivos elencados para a aplicação da tecnologia; (ii) que perspetivas foram consideradas na decisão política; (iii) as vantagens e riscos da tecnologia que são descritos; bem como, (iv) as suas limitações técnicas e operacionais (Wienroth, 2020). Neste caso, dado que o *Big Data* para fins de previsão criminal não apresenta um enquadramento legislativo específico (Neiva & Machado, 2021), os documentos regulatórios considerados são o Regulamento Geral da Proteção de Dados da União Europeia 2016/679 (RGPD) e a Diretiva Europeia 2016/680 sobre o tratamento de dados pessoais na prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções. A legitimidade das tecnologias deve considerar a análise dos propósitos da sua implementação, bem como, refletir sobre, por exemplo, em que tipo de crimes a sua utilização é considerada legítima (Wienroth, 2020). No caso de *Big Data*, este aplica-se a "infrações graves" (Diretiva 2016/680), mas deve refletir-se sobre quais são os catálogos criminais aqui contemplados (Neiva & Machado, 2021).

13 Tradução portuguesa do conceito *Responsible Research Innovation*.

A deliberação em torno da legitimidade de *Big Data* inclui, também, realizar avaliações frequentes à sua aplicação, dado que, não raras vezes, a implementação das tecnologias pode conduzir a situações de desrespeito de direitos humanos (Wienroth, 2020). Por exemplo, no âmbito de *Big Data*, por via da análise da Diretiva 2016/680, podemos aferir de desafios diversos (Neiva & Machado, 2021). Nomeadamente, a transferência de dados sobre infrações graves não apresenta restrições de acesso; o direito de acesso aos dados por parte do titular pode ser negado (artigo 15.º, Diretiva 2016/680); e relativamente ao consentimento, a Diretiva 2016/680 não prevê normas para o seu exercício (Neiva & Machado, 2021). Para que estas situações sejam analisadas, é necessário que seja feita uma fiscalização e supervisão do uso de *Big Data* na previsão criminal, por órgãos independentes, como é o caso da Comissão Nacional de Proteção de Dados e o Comité (artigo 51.º Diretiva 2016/680) responsável pela avaliação dos impactos das tecnologias na proteção de dados. Estas entidades devem prever valores éticos a serem salvaguardados na utilização de *Big Data* para fins de previsão criminal (Neiva & Machado, 2021).

5. Conclusão

Este texto pretendeu refletir sobre o modo como a tecnologia de *Big Data* (re)produz potenciais impactos na sua aplicação, que tipos de danos desencadeia, sobre quem atuam e de que forma, estendendo a reflexão à elaboração de um conjunto de propostas que visam, além de fomentar debates públicos em torno das novas tecnologias, antecipar e minimizar os efeitos sociais negativos decorrentes da sua aplicação.

Considerando os "efeitos de desempoderamento" como o conjunto de consequências negativas que estes sistemas automatizados provocam no tecido social, com repercussões na confiança e democracia, responsabilização e transparência, inclusão e igualdade social, propomos um conjunto de práticas com potencial para os mitigar. As enunciações que elaboramos visam, a um nível geral, promover a governação da tecnologia de *Big Data*, democratizando-a e encorajando os polícias, legisladores, políticos e outros *stakeholders* a consciencializarem-se sobre os dados. Ao considerar a robustez, a utilidade e a legitimidade (Wienroth, 2020) como valores-chave na deliberação das tecnologias, incorporamos princípios que superam as tradicionais preocupações técnicas em torno das capacidades, eficácia e eficiência de *Big Data* na previsão criminal. Este conjunto de estratégias visam uma implementação transparente, ética e inclusiva de *Big Data* neste contexto, fomentando a confiança dos cidadãos nas instituições governamentais, tornando-os parte ativa dos processos de *design* e aplicação das tecnologias. Além dos cidadãos, refletimos sobre a inclusão de diferentes públicos, desde profissionais que desenvolvem os *softwares*, aos que a utilizam, avaliam e legitimam.

Privilegiando uma comunicação clara e transparente, estas estratégias têm potencial para minimizar as consequências sociais negativas enraizadas decorrentes do uso

de novas tecnologias para fins de segurança. No entanto, esta deliberação interdisciplinar pode tornar-se um desafio quando a validação material da tecnologia é valorizada em detrimento de outras considerações. Por exemplo, a conceção generalizada de que qualquer ferramenta tecnológica que auxilie na apreensão de um perpetrador criminal deve ser implementada, independentemente das suas limitações e impactos sociais (Wienroth, 2020).

O tempo dirá se este conjunto de estratégias poderão, efetivamente, contribuir para uma implementação de *Big Data* na previsão criminal mais inclusiva, ética e transparente. No entanto, tal como Guston (2014, p. 218) reflete acerca da governação antecipatória das tecnologias, "podem não ser soluções para os nossos problemas em governar a tecnologia, mas certamente podem contribuir para uma aplicação da tecnologia norteada para fins humanos". Como refletimos, a eficácia de *Big Data* na previsão criminal não está comprovada, enquanto que vários países estão a investir em novas tecnologias para prever o crime (Jackson *et al.*, 2014; Nationale Politie, 2015; College of Policing, 2016). Estas reflexões denotam que, ao invés de se investir em estratégias que promovam debates em torno da robustez, utilidade e legitimidade das tecnologias nos contextos de aplicação da lei, investe-se em tecnologias que, além de não terem provado a sua eficácia (Meijer & Wessels, 2019), demonstraram ter "efeitos de desempoderamento" nos indivíduos, grupos e sociedades. Citando Van Brakel (2021, p. 237) "como as revelações de Snowden indicaram, a violação de direitos parece ser uma tarefa fácil, mas restaurá-los e reconquistar a confiança dos cidadãos demora muito mais tempo".

Grande parte da literatura académica das ciências sociais sobre *Big Data* na previsão criminal tem como foco os efeitos sociais negativos da sua aplicação. No entanto, esta centralização não permite a reflexão em torno de considerações sobre o facto da tecnologia poder ser implementada com motivações diferentes, incluindo um público vasto de atores sociais como a que foi exposta neste texto. O objetivo é potenciar a capacidade da sociedade debater valores públicos no contexto da emergência de novas tecnologias. A compreensão de uma diversidade de perspetivas sobre *Big Data* na previsão criminal pode contribuir para antecipar e avaliar as suas potenciais implicações éticas e sociais, seguindo os princípios da Investigação e Inovação Responsáveis (RRI) (Betten *et al.*, 2018; Yu, 2016). Consideramos, portanto, que a inclusão de uma nova tecnologia requer um debate público diversificado, transparente e inclusivo, especialmente, no caso de *Big Data* na previsão criminal, quando se trata de utilizar a tecnologia para informar decisões de natureza criminal.

Agradecimentos

Este trabalho recebeu financiamento nacional da Fundação para a Ciência e Tecnologia no âmbito de uma bolsa individual de doutoramento concedida a Laura Neiva [referência de bolsa 2020.04764.BD].

Bibliografia

Andrejevic, M., Dencik, L., & Treré, E. (2020). From pre-emption to slowness: assessing the contrasting temporalities of data-driven predictive policing. *New Media & Society*, 22(9), 1528–1544. https://doi.org/10.1177/1461444820913565

Aradau, C. (2015). The signature of security: *Big Data*, anticipation, surveillance. *Radical Philosophy*, *191*, 21-28.

Aradau, C., & Blanke, T. (2015). The (Big) Data-security assemblage: knowledge and critique. *Big Data & Society*, *2*(2), 1-12. https://doi.org/10.1177/2053951715609066

Aradau, C., & Blanke, T. (2017). Politics of prediction: security and the time/space of governmentality in the age of *Big Data*. *European Journal of Social Theory*, *20*(3), 373-391. https://doi.org/10.1177/1368431016667623

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. *Big Data & Society*, *6*(1), 1-13. https://doi.org/10.1177/2053951719861703

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

Berk, R., Sherman, L., Barnes, G., Kurtz, E., & Ahlman, L. (2009). Forecasting murder within a population of probationers and parolees: a high stakes application of statistical learning. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, *172*(1), 191–211. https://doi.org/10.1111/j.1467-985X.2008.00556.x

Betten, A. W., Rerimassie, V., Broerse, J. E., Stemerding, D., & Kupper, F. (2018). Constructing future scenarios as a tool to foster responsible research and innovation among future synthetic biologists. *Life Sciences, Society and Policy*, *14*(1), 1-20. https://doi.org/10.1186/s40504-018-0082-1

Bijker, W. E., & Law, J. (Eds.). (1994). *Shaping technology/building society: Studies in sociotechnical change*. MIT press.

Brayne, S. (2014). Surveillance and system avoidance: criminal justice contact and institutional attachment. *American Sociological Review*, *79*(3), 367-391. https://doi.org/10.1177/0003122414530398

Brayne, S. (2017). *Big Data* surveillance: the case of policing. *American sociological review*, *82*(5), 977-1008. https://doi.org/10.1177%2F0003122417725865

Browning, M., & Arrigo, B. (2021). Stop and risk: policing, data, and the digital age of discrimination. *American Journal of Criminal Justice*, *46*(2), 298-316. https://doi.org/10.1007/s12103-020-09557-x

Chan, J., & Moses, L. (2017). Making sense of *Big Data* for security. *The British Journal of Criminology*, *57*(2), 299-319. https://doi.org/10.1093/bjc/azw059

College of Policing (2016). *National Policing Vision*. United Kingdom. www.college.police.uk/About/Pages/National-policing-vision-2016.aspx

Dencik, L., Hintz, A., & Carey, Z. (2018). Prediction, pre-emption and limits to dissent: social media and *Big Data* uses for policing protests in the United Kingdom. *New Media & Society*, *20*(4), 1433–1450. https://doi.org/10.1177/1461444817697722

Diretiva da União Europeia de 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Retirado de: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680

Egbert, S. (2019). Predictive policing and the platformization of police work. *Surveillance & Society*, *17*(1/2), 83–88. https://doi.org/10.24908/ss.v17i1/2.12920

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

Einsiedel, E. F., & Eastlick, D. L. (2000). Consensus conferences as deliberative democracy: a communications perspective. *Science Communication, 21*(4), 323-343. https://doi.org/10.1177/1075547000021004001

Ferguson, A. (2015). *Big Data* and predictive reasonable suspicion. *University of Pennsylvania Law Review, 163*(2), 327-410.

Guston, D. H. (2014). Understanding 'anticipatory governance'. *Social Studies of Science*, *44*(2), 218-242. https://doi.org/10.1177/0306312713508669

Hardyns, W., & Rummens, A. (2018). Predictive policing as a new tool for law enforcement? Recent developments and challenges. *European Journal on Criminal Policy and Research*, *24*(3), 201–218. https://doi.org/10.1007/s10610-017-9361-2

Jackson, B.A., Greenfield, V. A., Moral, A. R., & Hollywood, J.S. (2014). *Police department investments in information technology systems*. Rand Research Report. Santa Monica, CA: RAND Corportation. www.rand.org/pubs/research_reports/rr569.html

Joh, E. E. (2014). Policing by numbers: *Big Data* and the Fourth Amendment. *Washington Law Review*, *89*, 35-68.

Joh, E. E. (2016). The new surveillance discretion: automated suspicion, *Big Data*, and policing. *Harvard Law & Pol'y Rev*iew, 10, 15-42.

Johnson, R. A., & Rostain, T. (2020). Tool for surveillance or spotlight on inequality? *Big Data* and the law. *Annual Review of Law and Social Science*, *16*(1), 453–472. https://doi.org/10.1146/annurev-lawsocsci-061020-050543

Kaufmann, M., Egbert, S., & Leese, M. (2019). Predictive policing and the politics of patterns. *The British Journal of Criminology*, *59*(3), 674–692. https://doi.org/10.1093/bjc/azy060

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big data & Society*, *1*(1), 1-12. https://doi.org/10.1177/2053951714528481

Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016). How we analyzed the COMPAS recidivism algorithm. *ProPublica (5 2016)*, *9*(1).

Leese, M. (2014) The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue, 45*(5), 494-511. https://doi.org/10.1177/0967010614544204

Lei, C. (2019). Legal control over *Big Data* criminal investigation. *Social Sciences in China*, *40*(3), 189-204. https://doi.org/10.1080/02529203.2019.1639963

Lyon, D. (Ed.). (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, D. (2014). Surveillance, Snowden, and *Big Data*: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1-13. https://doi.org/10.1177/2053951714541861

Machado, H., & Frois, C. (2014). Aspiring to modernization: historical evolution and current trends of state surveillance in Portugal. In Boersma, K., van Brakel, R., Fonio, C., & Wagenaar, P. (Eds.). *Histories of State surveillance in Europe and beyond* (pp. 65-78). United Kingdom: Routledge. https://doi.org/10.4324/9780203366134

Marciani, G., Porretta, M., Nardelli, M., & Italiano, G. F. (2017). A data streaming approach to link mining in criminal networks. *Proceedings of the 5th International Conference on Future Internet of Things and Cloud Workshops,* 138-143. https://doi.org/10.1109/FiCloudW.2017.88

Masadeh, M. A. (2012). Focus group: reviews and practices. *The Journal of Applied Science and Technology*, *2*(10), 63-68.

Matzner, T. (2016). Beyond data as representation: the performativity of *Big Data* in surveillance. *Surveillance and Society*, *14*(2), 197–210. https://doi.org/10.24908/ss.v14i2.5831

Meijer, A., & Wessels, M. (2019). Predictive policing: review of benefits and drawbacks. *International Journal of Public Administration*, *42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 1-15. https://doi.org/10.1177%2F2053951720948087

Minocher, X., & Randall, C. (2020). Predictable policing: new technology, old bias, and future resistance in *Big Data* surveillance. *Convergence: The International Journal of Research into New Media Technologies*, *26*(5–6), 1108–1124. https://doi.org/10.1177/1354856520933838

Monahan, T. (2010). Surveillance as governance: social inequality and the pursuit of democratic surveillance. In Kevin D. Haggerty, & Minas Samatas (Eds.). *Surveillance and Democracy* (pp. 91-110). Routledge.

Nationale Politie (2015). *Begroting Nationale Politie 2016-2020*. www.rijksoverheid.nl/documenten/begrotingen/2015/09/15/begroting-nationale-politie-2016

Neiva, L. (2020). *Big Data na Investigação Criminal: Desafios e Expectativas na União Europeia*. Editora Húmus.

Neiva, L. (2021). Big Data e vigilância policial: desafios éticos, sociais e legais. In Machado, H. (Ed.). *Crime e Tecnologia: Desafios Culturais e Políticos para a Europa* (pp. 65-80). Edições Afrontamento.

Neiva, L., & Machado, H. (2021). Big Data na investigação criminal: "Imaginário Europeu" e orientações para o futuro. In *E-Book II Jornadas Doutorais em Sociologia "Ciência & Política: Fronteiras e Intersecções"* (pp. 28-41). Departamento de Sociologia, Instituto de Ciências Sociais da Universidade do Minho.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

Plaksiy, K., Nikiforov, A., & Miloslavskaya, N. (2018). Applying *Big Data* technologies to detect cases of money laundering and counter financing of terrorism. *Proceedings of 6th International Conference on Future Internet of Things and Cloud Workshops,* 70-77). https://doi.org/10.1109/W-FiCloud.2018.00017

Pramanik, M. I., Lau, R. Y. K., Yue, W. T., Ye, Y., & Li, C. (2017). *Big Data* analytics for security and criminal investigations. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(4), e1208. https://doi.org/10.1002/widm.1208

Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Retirado de: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Ratcliffe, J. (2014). What Is the Future... of Predictive Policing? *Translational Criminology*, (6), 4–5.

Van Brakel, R. (2016). Pre-emptive *Big Data* surveillance and its (dis)empowering consequences: The case of predictive policing. In Sloot, B., Broeders, D., & Schrijvers, E. (Eds.). *Exploring the Boundaries of Big Data* (pp. 117-141). Amsterdam University Press.

Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies. In De Pauw, E., Ponsaers, P., Bruggeman, W., Van Der Vijver, K., & Deelman, P. (Eds.). *Technology-Led Policing* (pp. 165-192). Maklu.

Van Brakel, R. (2021). How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. *Surveillance & Society*, *19*(2), 228-240. https://doi.org/10.24908/ss.v19i2.14325

Sanders, C., Christensen, T., & Weston, C. (2015). Constructing crime in a database: *Big Data* and the mangle of social problems work. *Qualitative Sociology Review*, *11*(2), 180–195.

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

Završnik, A. (2019). Algorithmic justice: algorithms and *Big Data* in criminal justice settings. *European Journal of Criminology*, *1*(20), 623-642. https://doi.org/10.1177/1477370819876762

Wienroth, M. (2020). Value beyond scientific validity: let's RULE (Reliability, Utility, LEgitimacy). *Journal of Responsible Innovation*, *7*(sup1), 92-103. https://doi.org/10.1080/23299460.2020.1835152

Yu, H. (2016). Redefining responsible research and innovation for the advancement of biobanking and biomedical research. *Journal of Law and the Biosciences*, *3*(3), 611-635. https://doi.org/10.1093/jlb/lsw047