

Capítulo VI

Opacidade e Responsabilização nas Infraestruturas Digitais Policiais: Desafios Sociotécnicos em Contextos Institucionais Portugueses

Opacity and Accountability in Policing Digital Infrastructures: Sociotechnical Challenges within Portuguese Institutional Settings

Laura Neiva

Faculdade de Direito da Universidade Lusíada — Porto, Portugal; Centro de Estudos Jurídicos, Económicos e Ambientais (CEJEIA) da Universidade Lusíada; Departamento de Sociologia, Instituto de Ciências Sociais da Universidade do Minho, Braga, Portugal; Centro de Estudos de Comunicação e Sociedade da Universidade do Minho, Braga, Portugal

Resumo: A crescente incorporação de infraestruturas digitais no domínio policial, nomeadamente aquelas baseadas em tecnologias de *Big Data*, tem sido acompanhada por narrativas de modernização institucional, orientadas por promessas de eficácia, previsibilidade e racionalização da ação. No entanto, estas tecnologias não operam de forma neutra: são artefactos sociotécnicos que introduzem camadas significativas de opacidade nos processos decisórios, desafiando os mecanismos tradicionais de responsabilização institucional. Este capítulo propõe uma análise crítica da relação entre opacidade e responsabilização no contexto das infraestruturas digitais policiais em Portugal, com base numa investigação desenvolvida junto da Polícia Judiciária (PJ) e da Polícia de Segurança Pública (PSP). Mobilizando os contributos dos Estudos Sociais da Ciência e Tecnologia (STS) e da Sociologia das Expectativas, explora-se de que modo estas infraestruturas se tornam “caixas negras” tecno políticas, como são apropriadas discursivamente pelos profissionais da polícia, e que desafios colocam à transparência, à governança algorítmica e à prestação de contas em regimes democráticos. Argumenta-se que a responsabilização institucional requer mais do que dispositivos técnicos de auditoria: exige práticas reflexivas, marcos regulatórios robustos e mediações sociopolíticas que reinscrevam a responsabilidade nos processos sociotécnicos contemporâneos.

Palavras-chave: *big data*, policiamento, opacidade, responsabilização, infraestruturas digitais, sts

Abstract: The growing incorporation of digital infrastructures in policing, particularly those based on Big Data technologies, has been accompanied by institutional modernization narratives framed by promises of efficiency, predictability, and rationalization. However, these technologies do not operate in a neutral or transparent fashion: they are sociotechnical artefacts that introduce significant layers of opacity into decision-making processes, thereby challenging conventional mechanisms of institutional accountability. This chapter offers a critical analysis of the relationship between opacity and accountability in the context of digital policing infrastructures in Portugal, drawing on empirical research conducted within the Judiciary Police (PJ) and the Public Security Police (PSP). Anchored in the theoretical contributions of Science and Technology Studies (STS) and the Sociology of Expectations, the chapter examines how these infrastructures become technopolitical “black boxes”, how they are discursively appropriated by police professionals, and the challenges they pose to transparency, algorithmic governance, and democratic accountability. It is argued that institutional accountability requires more than technical auditing mechanisms: it necessitates reflexive practices, robust regulatory frameworks, and sociopolitical mediations that re-inscribe responsibility into contemporary sociotechnical processes.

Keywords: big data, policing, opacity, accountability, digital infrastructures, sts

Introdução

As infraestruturas digitais tornaram-se elementos centrais no funcionamento contemporâneo das instituições públicas, moldando não apenas os modos de produção de informação, mas também os processos de decisão, a distribuição de responsabilidades e as dinâmicas de poder (Ozili, 2025). Na segurança pública, estas transformações são particularmente significativas. A crescente adoção de *Big Data* — tecnologias com capacidades de acesso, recolha, análise e processamento de grandes volumes de dados — por forças policiais tem sido justificada por promessas de eficiência, rapidez, previsibilidade e racionalidade (Neiva, Machado & Silva, 2023). Contudo, tais promessas não operam num vazio político ou institucional: são performativas, ideologicamente orientadas e materialmente situadas (Neiva, 2024).

Este capítulo parte do pressuposto de que as infraestruturas digitais não são meros instrumentos técnicos, mas sim “caixas negras” (Latour, 1987, p. 3), cuja análise exige atenção às suas condições de produção, apropriação e circulação. O conceito refere-se ao modo como a complexidade das tecnologias é invisibilizada no seu uso quotidiano, sendo tratadas como funcionais e opacas. A sua “caixa negra” só se abre quando ocorre falha, conflito ou contestação. Em particular, interessa aqui compreender os efeitos sociopolíticos da opacidade que estas tecnologias introduzem nos sistemas policiais — como um regime institucional e organizacional que dificulta o escrutínio, desloca a responsabilidade e consolida formas de autoridade não deliberativa (Wessels, 2024).

Num contexto global de crescente confiança na automação e na governança algorítmica, o campo policial surge como um espaço privilegiado para observar os efeitos concretos dessas infraestruturas, seja nas práticas quotidianas dos profissionais, seja nos discursos institucionais que legitimam a sua adoção. Em Portugal, embora os estudos sobre digitalização policial sejam escassos, as transformações em curso evidenciam tendências semelhantes às observadas noutras geografias: crescimento da vigilância orientada por dados, reorganização de fluxos de informação, e expansão de lógicas de gestão tecnocrática do risco (Amoore, 2020).

A análise desenvolvida neste capítulo assenta numa investigação qualitativa realizada junto de profissionais da Polícia Judiciária (PJ) e da Polícia de Segurança Pública (PSP), tendo como objetivo compreender como são experienciadas, interpretadas e apropriadas as tecnologias de *Big Data*. Com base em entrevistas semiestruturadas e nos Estudos de Ciência, Tecnologia e Sociedade (STS), propõe-se um olhar crítico sobre três dimensões: (i) as expectativas performativas em torno das tecnologias, (ii) os processos de fragmentação da responsabilidade e da agência, e (iii) a presença de uma transparência seletiva.

Ao centrar-se no caso português, o capítulo pretende contribuir para um mapeamento empírico de um contexto pouco explorado, dialogando, ainda com debates teóricos mais amplos sobre governança algorítmica, opacidade institucional e responsabilização (Coglianese & Lehr, 2019; Philip, 2009).

Antecedentes da Digitalização Policial em Portugal

A digitalização das forças policiais em Portugal inscreve-se num processo mais amplo de modernização da administração pública, iniciado nas décadas de 1990 e 2000 (Silva, 2022). Esta trajetória foi marcada, num primeiro momento, pela informatização de registos e pela criação de bases de dados criminais internas, com a implementação de sistemas como o SEI (Sistema Estratégico de Informação), utilizado pela PSP (Morgado & Felgueiras, 2021; Morgado, Felgueiras & Moura, 2024; Pereira, 2019), e de plataformas de gestão investigativa próprias da PJ (Miranda, 2019). Esses sistemas visavam uma maior eficiência burocrática e a melhoria dos fluxos internos de informação.

A partir da década de 2010, com a emergência de programas europeus como o Horizonte 2020¹ e a crescente securitização das políticas migratórias e de fronteiras, intensificaram-se as iniciativas de desenvolvimento tecnológico orientadas para a vigilância preditiva, o policiamento baseado em risco e a interoperabilidade entre bases de dados criminais (Sánchez-Monedero & Dencik, 2022). Neste período, a modernização passou a ser também uma resposta a exigências externas (Machado & Frois, 2014), estruturando-se em torno da ideia de inovação como sinónimo de legitimação institucional: “a modernização possibilitada pela tecnologia (...) e a necessidade de desenvolvimento contrastam, em termos de discurso político, com o reconhecimento de um atraso, um certo ‘complexo de inferioridade’ e uma perceção da condição periférica e atrasada de Portugal” (Miranda, 2019, p. 6; ver, também, Nunes & Gonçalves, 2001; Frois, 2013).

No caso da PJ, a evolução tecnológica desde os arquivos em papel e as máquinas de escrever, até sistemas de armazenamento de dados policiais mais aprimorados, a novos meios de transporte e de comunicação, bem como, de estratégias digitais de partilha de informação criminal (Miranda, 2019), ocorreu de forma gradual, acompanhando as tendências mais amplas de modernização. No caso da PSP, a adoção de bases de dados tornou-se um instrumento importante para a polícia, sendo que “a informatização do sistema de recolha, registo e partilha interna da informação policial [se tornou um] processo cada vez mais generalizado” (Durão, 2008, p. 204). Além disso, a adoção pelas forças policiais em Portugal do *i2 Analyst’s Notebook* — um *software* que organiza e visualiza dados de investigações criminais, mapeando relações entre pessoas, locais e eventos (Kubler, 2017) — demonstra a sua mobilização em torno da tecnologia. Estes avanços, muitas vezes financiados por fundos europeus, baseiam-se em lógicas de prevenção e eficiência. A estratégia digital da União Europeia (Comissão Europeia, 2023) aponta para o uso crescente de *Big Data*, prevendo-se a sua adoção também por instituições públicas, incluindo as policiais.

No entanto, estas transformações tecnológicas têm decorrido com escassa regulamentação específica sobre o uso de algoritmos em contextos coercivos, e sem debates públicos significativos (Neiva & Machado, 2022; Pereira, 2019). A ausência de transparência deliberativa sobre critérios técnicos, riscos discriminatórios e impactos nos direitos fundamentais levanta preocupações relevantes (Neiva & Machado, 2022). O quadro normativo nacional — adaptado às exigências do Regulamento Geral de Proteção de Dados através da Lei n.º 58/2019 — carece de dispositivos regulatórios robustos no que toca à aplicação de sistemas de decisão automatizada no setor da segurança (Neiva, 2023, 2024).

1 O *Horizonte 2020* foi o maior programa de investigação e inovação da União Europeia, em vigor entre 2014 e 2020, com um orçamento de cerca de 80 mil milhões de euros. Visava promover o desenvolvimento científico e tecnológico europeu, incluindo projetos nas áreas da segurança, vigilância, policiamento e controlo de fronteiras, sob o pilar “Sociedades Seguras” (União Europeia, s.d.).

Esta configuração reforça a importância de compreender o caso português como um espaço onde se jogam disputas sobre soberania tecnológica, responsabilização democrática e imaginação institucional do futuro da segurança pública.

Infraestruturas Digitais Policiais como Caixas Negras Sociotécnicas

As infraestruturas digitais devem ser entendidas enquanto artefactos sociotécnicos que integram elementos técnicos, institucionais, simbólicos e humanos (Monteiro & Hanseth, 1996). Tal como propõem Bijker e Law (1992), as tecnologias não são objetos neutros ou acabados, mas constituem-se nas redes heterogêneas que as produzem, mantêm e legitimam. No campo da segurança pública, estas redes envolvem não apenas engenheiros e programadores, mas também decisores políticos, profissionais da polícia, quadros jurídicos e imaginários sociais sobre segurança, risco e controlo. Esta perspetiva desafia as concepções funcionalistas e deterministas da tecnologia, propondo que as infraestruturas digitais são simultaneamente moldadas e moldadoras das práticas sociais que as envolvem (Jasanoff, 2004). Em vez de instrumentos estáticos, operam como configurações sociotécnicas (Law, 2008), nas quais se inscrevem dinâmicas de poder, modos de governação e formas de exclusão.

Neste contexto, a opacidade torna-se um conceito chave. Como argumenta Latour (1987, p. 3), as tecnologias, ao tornarem-se estáveis e institucionalizadas, tendem a funcionar como “caixas negras”: dispositivos cuja complexidade interna é ocultada pelos seus produtores, provocando efeitos que são simultaneamente naturalizados e despolitizados. No caso das infraestruturas digitais policiais, esta opacidade manifesta-se de várias formas: algoritmos cujo funcionamento é inacessível, externalizações contratuais que fragmentam a cadeia de responsabilidade, e culturas organizacionais que privilegiam o sigilo em detrimento da transparência. Os programas informáticos de previsão criminal² carecem de transparência quanto à criação de perfis “suspeitos”, à definição de ameaças e à programação dos algoritmos (Van Brakel, 2016; Van Brakel & Govaerts, 2024). Os processos de inserção de dados nos softwares e a forma como os algoritmos (re)definem categorias são pouco transparentes, já que as empresas raramente divulgam como essas tecnologias foram desenvolvidas ou como os dados são obtidos e armazenados. Tal como o sociólogo Latour (2010, p. 26) referiu, “o objeto tecnológico é opaco, e — para dizer sem rodeios — incompreensível”.

2 Por exemplo no caso do *PredPol*, um sistema que usa dados criminais passados para criar mapas de frequência criminal (Hardyns & Rummens, 2018), os algoritmos são inseridos pelo fabricante, o que revela a falta de transparência sobre os dados usados nas previsões criminais (Oatley, 2022; Van Brakel & Govaerts, 2024).

Não obstante, a emergência de tecnologias é frequentemente acompanhada por expectativas performativas que estruturam antecipadamente as suas trajetórias de desenvolvimento (Borup *et al.*, 2006). No caso português, o discurso da inevitabilidade tecnológica atravessa as narrativas institucionais sobre *Big Data*, construindo um futuro desejável onde a tecnologia surge como resposta natural e objetiva a problemas estruturais do sistema de justiça criminal (Neiva, 2024). Estas expectativas, ao mesmo tempo que legitimam investimentos e reorganizações, obscurecem as implicações éticas, sociais e políticas do uso dessas tecnologias (Neiva, 2023).

Neste capítulo sustenta-se que esta opacidade não é um efeito colateral, mas uma característica constitutiva das infraestruturas digitais desenhada, mantida e justificada como parte do seu funcionamento. A responsabilização institucional torna-se, assim, um processo fragmentado, diluído entre entidades técnicas, departamentos jurídicos, protocolos operacionais e lógicas algorítmicas que escapam ao controlo direto dos agentes humanos implicados na decisão. Tal cenário exige uma abordagem crítica que articule a análise dos dispositivos técnicos com os contextos institucionais e discursivos em que estes são apropriados, contestados ou naturalizados.

Infraestruturas Digitais, Opacidade e Responsabilização: Um Olhar Ampliado

As infraestruturas digitais, particularmente em domínios de governação como o policiamento, devem ser compreendidas como redes sociotécnicas densas que integram materialidades tecnológicas, regimes institucionais, dispositivos discursivos e práticas normativas. Uma infraestrutura não é apenas um suporte técnico, mas uma ecologia de relações que ganha visibilidade quando falha ou se torna objeto de disputa (Star & Ruhleder, 1996).

No contexto do policiamento digital, a opacidade não deve ser lida como um “acidente de percurso”, mas como uma característica constitutiva de certas racionalidades tecno políticas contemporâneas (Ananny & Crawford, 2018). Esta pode emergir de códigos proprietários, da complexidade computacional ou da fragmentação das responsabilidades institucionais, criando o que Pasquale (2015) denomina de sociedade de caixa-preta: uma sociedade em que as decisões são tomadas por sistemas opacos, sem que se conheçam os critérios que as fundamentam. Por sua vez, a responsabilização não é uma qualidade inerente aos sistemas técnicos, mas um regime de prática e discurso que se constrói institucionalmente. Como sublinham Schuppli (2014) e Amoores (2020), a auditabilidade dos algoritmos depende de condições epistemológicas e políticas que raramente estão garantidas, sobretudo em contextos securitários. A lacuna de responsabilização, ou seja, a ausência de clareza sobre quem é responsável por decisões automatizadas, dificulta a atribuição de responsabilidades e a supervisão ética ou legal desses sistemas, ampliando-se estas questões quando estes sistemas participam em decisões com impacto sobre os direitos, liberdades e garantias dos cidadãos (Lyon, 2007). Além disso, os estudos críticos da vigilância (Lyon, 2018; Zuboff, 2019) apontam para uma transformação profunda dos modos de governo, em que o controlo não se limita à supervisão visível, mas se inscreve em lógicas preditivas e antecipatórias.

Neste quadro, é necessário articular a crítica da opacidade com uma abordagem sociológica da responsabilização como prática situada, mediada por relações de poder, normas institucionais e imaginários de segurança.

Notas Metodológicas e Teórico-Analíticas

O capítulo baseia-se numa investigação qualitativa desenvolvida entre 2020 e 2024, no âmbito de um projeto de doutoramento³ centrado nas expectativas sobre *Big Data* por parte de profissionais da PJ e da PSP em Portugal. As missões e enquadramentos institucionais de ambas são distintos: a PJ, sob tutela do Ministério da Justiça, é responsável pela investigação criminal; a PSP, sob tutela do Ministério da Administração Interna, assegura o policiamento urbano. Estas duas forças policiais representam tendências potencialmente extensíveis a outras agências de segurança. O material empírico inclui 34 entrevistas semiestruturadas conduzidas com profissionais em exercício ativo das suas funções, selecionados de forma intencional e teórica. Seguiu-se um protocolo ético que incluiu consentimento informado, garantindo o anonimato e a confidencialidade em todas as fases da investigação.

Estas entrevistas foram analisadas através de uma metodologia inspirada na Teoria Fundamentada (Charmaz, 2006) e na análise situacional (Clarke, 2005), permitindo mapear dimensões emergentes como expectativas, opacidade e responsabilização. A natureza indutiva da análise e a escolha por um número reduzido de entrevistas aprofundadas privilegiam a compreensão densa de sentidos e práticas, mas não permitem generalizações extensivas. A intenção do estudo é compreensiva (Yin, 2011): interpretar dinâmicas institucionais invisíveis e contribuir para um olhar crítico sobre os processos de digitalização policial em Portugal. Reconhece-se, assim, que os resultados aqui apresentados não são representativos da totalidade das experiências policiais em Portugal, mas constituem pistas significativas para a compreensão dos modos como a tecnologia é vivida, negociada e, por vezes, contestada no seio das instituições securitárias.

A estratégia analítica integra os dados empíricos com o referencial da Sociologia das Expectativas (Borup *et al.*, 2006) e com os STS (Bijker & Law, 1992; Law, 1991, 2008; Pickering, 1992) cujo contributo é central para a problematização da opacidade sociotécnica. O recurso a este enquadramento justifica-se pela sua capacidade de desestabilizar pressupostos deterministas e de tornar visível a natureza relacional, contingente e co construída dos artefactos

3 Financiado pela FCT — Fundação para a Ciência e Tecnologia, I.P., — através da concessão de uma bolsa de doutoramento (referência 2020.04764.BD e DOI 10.54499/2020.04764.BD) com proveniência no orçamento nacional e no orçamento comunitário através do Fundo Social Europeu (FSE), e do projeto UIDB/00736/2020 (financiamento base) e UIDP/00736/2020 (financiamento programático).

tecnológicos. Esta estratégia analítica assumiu um compromisso entre o rigor da codificação sistemática e a abertura à complexidade dos sentidos emergentes nas narrativas recolhidas. A análise foi orientada por codificação aberta e axial, permitindo identificar categorias analíticas que refletem tanto continuidades quanto tensões emergentes no discurso profissional. Para efeitos deste capítulo, a análise centra-se em três dimensões fundamentais: (1) as expectativas performativas em torno das tecnologias; (2) os processos de fragmentação da responsabilidade e da agência; e (3) a presença de uma transparência seletiva.

Infraestruturas Policiais Digitais em Prática: Sentidos, Resistências e Opacidades

1. Expectativas Performativas em Torno das Tecnologias

A difusão de infraestruturas digitais nas organizações policiais tem sido acompanhada de discursos promissores que associam as tecnologias à inovação, eficiência e inevitabilidade (Neiva, 2023, 2024; Neiva, Machado & Silva, 2023). *Big Data* é frequentemente apresentado como solução neutra e necessária, justificada por lógicas de atualização institucional e competitividade internacional. Ainda assim, as expectativas policiais demonstram que, longe de uma aceitação homogênea, são objeto de apropriações ambivalentes e de experiências dissonantes no quotidiano profissional. É possível identificar diferentes camadas discursivas e práticas associadas às expectativas sobre *Big Data*. Seguem-se duas dessas dimensões: a naturalização da inovação tecnológica como inevitável, e a distância entre as promessas discursivas e os constrangimentos do uso quotidiano.

1.1 Tecnologia como Inevitabilidade Institucional

A implementação de tecnologias em instituições policiais é apresentada como um processo inexorável de modernização, uma exigência do “mundo atual”. Esta retórica da inevitabilidade é performativa: não apenas descreve a mudança, mas contribui para a sua legitimação, encerrando o debate sobre alternativas possíveis, e transparecendo processos de negociação socio-técnica da inovação (Schjølin, 2020).

“Eu acho que nós, polícia, estamos cada vez mais ligados à tecnologia e daí fazer sentido falar num *Big Data*. O futuro é a tecnologia! Acho que o caminho será por aí e até no futuro se poderá implementar um *Big Data* na polícia, como é aplicado noutros lados... A polícia tem de se render... A polícia vai ter de se adaptar à evolução da criminalidade... E se a criminalidade está a ir por aí a polícia também tem que ir...” (E18-PSP)

“Bem, esperamos que nunca aconteça, mas se um dia acontecesse uma catástrofe em Portugal nós andávamos à escura e se calhar só assim é que alguém olhava e via o que realmente precisamos... De novas ferramentas como o *Big Data* para acompanhar a evolução da criminalidade!” (E17-PSP)

Estas narrativas refletem uma aceitação fatalista da tecnologia. Tal como sugerem Borup e colegas (2006), as expectativas tecnológicas configuram desde logo a trajetória institucional, produzindo orientações e investimentos antes da concretização técnica ou da demonstração de eficácia da tecnologia. A ideia de “ficar para trás” evoca uma pressão de análise comparativa internacional, reforçando a adoção de soluções técnicas como imperativo estratégico (Oomen *et al.*, 2022). Esta inevitabilidade convoca formas de autoridade epistémica específicas, associadas ao discurso tecnocientífico e à gestão por indicadores, deslocando o centro da deliberação de critérios sociopolíticos para racionalidades instrumentais (Oomen *et al.*, 2022; Schiølin, 2020).

1.2. Descompasso entre Promessa e Prática

Apesar da retórica promissora que acompanha a introdução de *Big Data*, muitos profissionais expressam uma perceção de descompasso entre os benefícios anunciados e os resultados efetivamente experienciados nas suas rotinas operacionais.

“[*Big Data*] É informação... Parece-me uma boa ferramenta de trabalho... Se bem que a nível da polícia eu tenho algumas reservas, não é? Não sei até que ponto é que isso... Por exemplo, para quem está disponível? Para que é? Como é que a informação é trabalhada? Como é que é utilizado? Que tipo de informação é que vai ser carregada? É filtrado? Mas sim, se for com algumas reservas, parece-me algo positivo...” (E18-PSP)

“[*Big Data*] em termos de aplicação à investigação criminal e policiamento... Há muitos problemas associados com a sua aplicação no sistema de justiça criminal. E não me parece que seja algum dia de facto aplicado ou aplicável... Existe a questão técnica que não me parece... Há uma série de questões, quer de procedimentos padrão que possam ser verificáveis, com chaves de encriptação para garantir acessos e depois a sua reprodução sem alteração... Mas *Big Data* daria muito jeito! Porque eu não iria perder o tempo que já perdi a pesquisar semanas e semanas...” (E15-PJ)

“Essas previsões [de *Big Data*] podem não ser 100% seguras, não é?” (E2-PJ)

Estes excertos revelam como as infraestruturas digitais não são simplesmente adotadas — são apropriadas, reinterpretadas e, por vezes, resistidas no terreno (Brayne, 2017). A promessa

de automação e racionalização é confrontada com constrangimentos materiais (como dificuldades técnicas) e institucionais (como a resistência organizacional) (Babuta, 2017). A performatividade das expectativas colide com o quotidiano institucional, gerando frustração e ceticismo. Isso reforça o argumento de que as tecnologias não se instalam em terreno neutro, mas em contextos sociotécnicos que moldam e são moldados pela sua incorporação (Jasanoff, 2004; Star & Ruhleder, 1996).

2. Os Processos de Fragmentação da Responsabilidade e da Agência

A introdução de infraestruturas digitais baseadas em *Big Data* no campo policial não apenas reorganiza fluxos de informação, mas também reconfigura as condições de produção da responsabilidade institucional. Para efeitos da presente análise, a responsabilidade engloba duas dimensões: a organizacional e a individual. A organizacional enfatiza a direção e o controlo de políticas de policiamento. A individual refere-se à responsabilização face a regras legais individuais e atividades diárias. Ambas se fundem na prática pois as condutas micro dos profissionais de polícia são influenciadas pelas perspetivas e práticas macro e vice-versa (Jones, 2012). Neste contexto, esta torna-se uma prática fragmentada, opaca e, frequentemente, deslocada entre humanos e sistemas técnicos. Esta secção analisa duas dimensões dessa reconfiguração: a delegação algorítmica como forma de desresponsabilização, e os efeitos de infraestruturas opacas no quotidiano policial.

2.1. Delegação e Desresponsabilização Algorítmica

Com a incorporação de sistemas digitais nos processos de triagem, priorização ou orientação investigativa e policial, muitos profissionais percebem um deslocamento da tomada de decisão para os sistemas. Esta delegação algorítmica é frequentemente acompanhada de uma diluição das responsabilidades humanas (Dempsey *et al.*, 2023; Rowe & Muir, 2021) e surge simbolicamente representada em questões. Neste capítulo, estas últimas não se limitam à expressão de reservas técnicas, mas articulam uma expectativa estratégica sobre o futuro da tecnologia no campo policial. Ao questionarem como, porquê e com que critérios os dados serão utilizados, inscrevem-se num debate macrossocial sobre a legitimidade e as implicações do uso de *Big Data* em contextos de autoridade pública. Mesmo afirmações marcadas por incerteza — como “não sei” — funcionam como enunciados performativos (Sovacool *et al.*, 2020), capazes de atrair atenção institucional e convocar outros atores sociais para a co construção de soluções regulatórias (Geels & Smit, 2000).

“Eu acho que [*Big Data*] é muito positivo... Desde que consiga recolher o máximo de informação possível, desde que respeite umas regras... Desde que sejam respeitados

princípios de proporção, do propósito da recolha dos dados, da explanação dos métodos... Tem de ser bem explicado... Eu acho que é muito útil porque permite uma melhor investigação criminal, mais efetiva...” (E8-PJ)

“Não me choca nada o *Big Data*. Agora, a utilização indevida do conjunto desses dados é um problema. Tem que haver punições bastante severas para quem prevaricar senão ia ser um descalabro.” (E27-PSP)

Estas expectativas, embora projetadas como condição para a eficácia, revelam também os contornos institucionais da delegação algorítmica: uma aceitação condicional baseada em pressupostos normativos e garantias externas. As tecnologias são valorizadas pelo seu potencial de eficácia, mas apenas se acompanhadas de sistemas de vigilância legal, controlo de acessos e mecanismos de responsabilização externa.

Outros testemunhos explicitam como os sistemas técnicos podem funcionar como escudos de proteção institucional, dificultando a atribuição de responsabilidade. O sistema orienta, o humano executa mas sem controlo pleno nem clareza sobre os critérios subjacentes. Essa redistribuição assimétrica da agência transforma a responsabilização num processo difuso (Wessels, 2024).

“Se eu fizer esse tipo de coisas, de pedir todos os dados para usar só os que depois me interessam... E depois se der erro de quem é a culpa? A tecnologia é o bode expiatório. Ah, a culpa é do *Big Data*. Não é, não é. Isso seria encontrar uma saída fácil... Culpar a tecnologia.” (E6-PJ)

“Um erro que pode acontecer é confiar-se demasiado na máquina e depois leva a outra questão ainda mais grave... Que é a da responsabilidade por esse erro! Se é da máquina ou se é da pessoa ou de quem criou a máquina... E portanto tem que se assegurar que a responsabilidade, do meu ponto de vista, é sempre humana.” (E8-PJ)

Esta fragmentação da agência entre humanos e sistemas técnicos desafia conceções lineares de causalidade e favorece a produção de zonas de indeterminação institucional. Os regimes de opacidade algorítmica não são apenas técnicos, mas também organizacionais e políticos, servindo para estabilizar assimetrias de poder (Ananny & Crawford, 2018). Além disso, a responsabilização torna-se reativa e não preventiva: só após a ocorrência de falhas se tenta reconstruir a cadeia decisória, frequentemente com escassos resultados.

Não obstante, o que também agrava a dificuldade de responsabilização são as fragilidades materiais e jurídicas das infraestruturas digitais. A natureza distribuída, imaterial e, por vezes, opaca do armazenamento e processamento de dados é apontada como um risco adicional.

“Os dados guardados na *cloud computing*... Ninguém nos garante que estão lá... É muito difícil arcar responsabilidades. A informação consta lá? É mantida nos termos

em que precisamos? Principalmente do ponto de vista processual penal, é de uma fragilidade enorme...” (E15-PJ)

Estas fragilidades técnicas associam-se a uma exigência recorrente entre os profissionais: a necessidade de reforçar dispositivos institucionais de controlo e responsabilização, como conselhos reguladores ou gabinetes de auditoria interna.

“Restringir... Por exemplo, à semelhança das interceções telefónicas... Criar um organismo que seja um conselho do *Big Data* com alguém responsável por controlar os acessos.” (E14-PJ)

Tal como propõem Borup e colegas (2006, p. 290), as expectativas tecnológicas operam entre a liberdade para imaginar e a obrigação social de concretizar. Neste caso, essa obrigação projeta-se na necessidade de mecanismos institucionais que reinscrevam a responsabilidade humana num ecossistema técnico cada vez mais distribuído.

2.2. Infraestruturas Invisíveis, Consequências Visíveis

Outro aspeto central emergente nas entrevistas prende-se com o modo como a opacidade se manifesta na estrutura técnica das infraestruturas, designadamente na origem, atualização e interoperabilidade dos dados, e nos efeitos concretos que daí resultam para o trabalho policial.

“O erro é gravíssimo e na prevenção criminal, um erro de análise pode levar a um acidente grave. Estamos a falar de forças policiais que usam armas com potencial operacional e que pode originar um problema, um acidente muito grave... Portanto a informação tem que ser muito bem tratada e esses erros podem-se pagar caros... Imagine o que é um erro sobre um indivíduo e o indivíduo estar a ser abordado e não ter nada a ver com aquilo... Porque a polícia com base em informação errada avança para esse objetivo, o indivíduo tem uma reação... E depois? Aí acabava-se logo com o *Big Data*.” (E27-PSP)

“Acredito que devido à velocidade de processamento, essas probabilidades calculadas pelo *software* [*Big Data*] são muito mais próximas da realidade do que se calhar um investigador criminal faria... A questão está na utilização destes resultados finais, porque uma das coisas que ganhei com 20 anos de experiência é que 90% das vezes é o que parece, ou até mais... 95% das vezes é o que parece... O problema são os outros 5%... E aquilo que fico sempre com receio relativamente a *Big Data* é esses 5%. Esse resto... E atenção que eu não estou a dizer que nós humanos fazemos melhor... Mas isto preocupa-me...” (E5-PJ)

Estes testemunhos revelam uma desarticulação entre a materialidade técnica dos sistemas e as exigências operacionais do terreno. A responsabilidade pela fiabilidade dos dados — elemento fundamental para a tomada de decisão — encontra-se diluída entre múltiplos departamentos e fornecedores externos, o que enfraquece as condições institucionais de escrutínio. Os algoritmos operam com lógicas de inferência que escapam à transparência linear (Amoore, 2020). No contexto policial, isso traduz-se em decisões que parecem racionais e automatizadas, mas cuja base epistémica e política permanece invisível para os utilizadores finais, reforçando a assimetria entre quem projeta, quem executa e quem é afetado.

“Tenho muita reserva [sobre *Big Data*]. Tem muitas variantes externas, muitas. Um *software* consegue prever indisposições que não colocam o suspeito no local previsto? Acontecimentos que atrasam crimes? Porque às vezes temos a certeza, por meios ocultos, que o crime vai acontecer depois de anos a investigar... E à última da hora não acontece... Há um conjunto de fatores que acho muito difícil um *software* prever... Que são fatores com base humana...” (E25-PSP)

Neste sentido, a fragmentação da agência e da responsabilidade compromete a própria lógica de responsabilização pública, dificultando a produção de respostas institucionais robustas perante falhas ou injustiças. Este processo de delegação parcial da agência para os sistemas configura aquilo que Bovens (2007) denomina responsabilização fragmentada, onde múltiplos atores partilham a responsabilidade sem que nenhum a assuma plenamente. Trata-se, assim, de um regime de governação que dificulta a imputação causal de consequências e favorece a produção de zonas de indeterminação institucional.

3. A Presença de uma Transparência Seletiva

A retórica institucional frequentemente invoca a transparência como princípio estruturante das práticas tecnológicas e organizacionais. Contudo, os dados empíricos indicam que essa transparência é seletiva, incompleta e muitas vezes circunscrita a lógicas internas de reporte vertical invisibilizando tanto os processos decisórios como os impactos para os próprios agentes e para o público. Esta secção desenvolve duas dimensões dessa problemática: os limites da transparência interna e a transformação da ética em retórica institucional.

3.1. Transparência, Ética e Relação com o Público

Entre os/as profissionais entrevistados/as, é recorrente a perceção de que as decisões sobre as tecnologias a adotar, bem como os critérios operacionais dos sistemas digitais, são tomadas por instâncias superiores, sem consulta nem partilha efetiva de informação com os utilizadores finais.

“Isso [para implementação de tecnologias de *Big Data* na polícia] é a nível político. São instituições e eles é que definem as regras, não somos nós [polícia].” (E31-PSP)

“Enquanto o governo não pensar conjuntamente connosco [polícia] e perceber... Eu gostava que antes de criarem uma lei viessem para o terreno, passassem uma semana no terreno connosco, com a PJ, PSP e GNR para perceberem como é que nós fazemos as coisas! Perceberem qual é a dificuldade e aí sim, depois criavam as leis direcionadas no sentido das necessidades...” (E16-PJ)

Estas narrativas evidenciam uma assimetria informacional estrutural. A transparência é exercida apenas na direção hierárquica descendente, limitada à entrega de resultados operacionais, sem abertura dos critérios, parâmetros ou lógicas algorítmicas que estruturam a produção dos resultados. Este modelo de transparência procedimental, mais do que democratizar o conhecimento sobre os sistemas, reforça a autoridade técnica e distancia os agentes da possibilidade de questionamento crítico (Kinchin, 2024).

A transparência, neste sentido, torna-se uma prática simbólica e mobilizada como valor institucional, mas esvaziada na sua concretização quotidiana. Tal como sugerem Ananny e Crawford (2018), tornar um sistema visível não é o mesmo que torná-lo compreensível, audível ou negociável.

3.2. Ética Como Retórica Institucional

As narrativas dos/as entrevistados/as revelam que os discursos institucionais sobre ética, embora recorrentes, são percecionados como abstratos, pouco práticos e exteriores à realidade operativa das polícias. A ética, nestas entrevistas, surge como linguagem performativa de legitimação, mas esvaziada de mecanismos concretos de deliberação e operacionalização. Tal como proposto por Green (2021), a “ética da tecnologia” deve ser analisada socio tecnicamente, interrogando quem define os seus contornos e com que efeitos. Neste caso, a invocação da ética pelas instituições policiais aparece como um recurso estratégico que visa, simultaneamente, acautelar o futuro e proteger a instituição da crítica pública.

“O RGPD veio trazer imensos problemas... Veio criar obstáculos que no futuro terão que ser ultrapassados... Compreendo a criação do RGPD, mas tem de haver exceções para fins de investigação criminal!” (E14-PJ)

“[Para aplicação de *Big Data* deveria existir] um protocolo institucional obrigatoriamente. E definir quem é que tem acesso ao quê... Que critérios é que permitem... Haver escalonamento! Quem tem acesso àquela informação?” (E5-PJ)

Estas declarações evidenciam a percepção de que os quadros normativos são concebidos à margem das práticas policiais, sendo impostos de forma distante e pouco ajustada à realidade operacional. Como tal, a ética surge como imposição normativa e não como construção coletiva.

“[O envolvimento da sociedade nestes temas de *Big Data* na investigação criminal e policiamento], de forma q.b.! Isto é sempre complicado... Devemos sim informar... Mas não precisam de saber como é que as coisas se fazem nos bastidores.” (E17-PSP)

Estas ambiguidades revelam como os discursos sobre a ética são frequentemente utilizados para reforçar a autoridade institucional e controlar os termos do debate público, em vez de promover um verdadeiro envolvimento dos cidadãos. Tal como analisado por Machado e Silva (2024), a instrumentalização das ideias é uma estratégia de tranquilização institucional perante incertezas futuras. Neste contexto, a ética converte-se num recurso retórico que permite às organizações afirmar compromisso público sem alterar significativamente as práticas ou abrir espaço à deliberação.

Esta configuração ética tecnocrática está longe de democratizar o conhecimento sobre os sistemas e tende, ao contrário, a reforçar a autoridade técnica, excluindo agentes e cidadãos da possibilidade de questionamento crítico (Bietti, 2021). Como argumentam Veale *et al.* (2018), a opacidade institucionalizada agrava as assimetrias entre quem concebe, quem aplica e quem é afetado pelos sistemas digitais, limitando o escrutínio social e jurídico.

Em suma, os discursos sobre a ética em torno de *Big Data* funcionam como uma forma de “fachada de ética” (Green, 2021, p. 212), legitimando a tecnologia sem criar espaços concretos para a sua regulação ou questionamento efetivo.

Opacidade, Agência e *Accountability* em Disputa: Desafios à Responsabilização e Caminhos para a Governação Democrática

A análise desenvolvida neste capítulo evidenciou que a adoção de infraestruturas digitais baseadas em *Big Data* no campo policial português está profundamente imbricada em dinâmicas de opacidade, reconfigurações do poder decisório e lógicas de desresponsabilização institucional. Os resultados apresentados permitem problematizar a relação entre inovação tecnológica e responsabilização institucional numa perspetiva relacional e crítica. Através das narrativas empíricas emergem três movimentos paralelos: (i) a naturalização das expectativas tecnológicas como inevitabilidade institucional; (ii) a fragmentação da agência e da responsabilidade entre humanos e sistemas técnicos; e (iii) a presença de uma transparência seletiva, que distancia tanto os profissionais como a sociedade civil dos critérios operacionais dos sistemas.

Estas dinâmicas remetem-nos para uma governação algorítmica caracterizada pela assimetria e pela opacidade intencional (Pasquale, 2015), que compromete os princípios de responsabilização democrática que asseguram que autoridades públicas prestem contas aos

cidadãos, com base na transparência, responsabilização e controlo democrático. A opacidade não é apenas uma limitação técnica, mas um dispositivo tecno político intencional, que reorganiza as condições da responsabilização institucional. Como defendem Latour (1992) e Jasanoff (2004), a agência humana não desaparece com a introdução dos sistemas algorítmicos, mas é redistribuída, reconfigurada e, por vezes, diluída em redes de decisão não transparentes. A responsabilização é deslocada, tornando mais difícil identificar responsáveis, auditar decisões ou corrigir erros. Essa arquitetura beneficia certos interesses organizacionais ao dificultar o escrutínio técnico e político (Pasquale, 2015). Na inexistência de mecanismos de participação e controlo externo, a ética transforma-se numa performance despolitizada, mais retórica do que substantiva (Machado & Silva, 2024).

Embora esta análise se foque no contexto português, as dinâmicas descritas têm ressonância internacional. Em países como os Estados Unidos, Reino Unido ou França, a incorporação de tecnologias digitais tem gerado regimes semelhantes de fragmentação da agência e erosão da responsabilidade (Brayne, 2017; Ferguson, 2018). No entanto, o caso português revela especificidades relevantes: a ausência de um debate público estruturado, a dependência de financiamento europeu e a fragilidade da regulação nacional constituem um cenário particularmente propício à legitimação silenciosa destas infraestruturas. As expectativas performativas sobre o *Big Data* enquanto promessa de eficácia e neutralidade produzem efeitos materiais nas políticas públicas e nas decisões organizacionais, mesmo antes da sua implementação efetiva (Borup *et al.*, 2006). Estas expectativas moldam discursos, atraem financiamento e justificam decisões estruturais, mesmo quando os sistemas ainda não funcionam plenamente ou revelam fragilidades operacionais (Konrad, 2006).

Face a este panorama, torna-se imperativo repensar as formas de governação algorítmica — um exercício de poder baseado em sistemas automatizados de decisão, em que algoritmos substituem ou orientam práticas humanas e deliberativas — à luz de princípios democráticos de responsabilização e coprodução (Bareis & Katzenbach, 2022). Não basta garantir a auditabilidade técnica dos sistemas. É necessário instituir práticas reflexivas que envolvam os próprios profissionais na definição de critérios de avaliação tecnológica, bem como mecanismos participativos que incluam representantes da sociedade civil, especialistas independentes e instâncias regulatórias robustas. Com base na análise apresentada, este capítulo recomenda a adoção de políticas públicas orientadas por quatro eixos centrais, sistematizados na tabela seguinte (ver Tabela 1):

Tabela 1

Eixos principais para orientação de políticas públicas

Eixo	Descrição
Transparência substantiva	Exigência de documentação acessível, explicabilidade algorítmica e mecanismos de comunicação pública sobre os sistemas utilizados, com base em modelos como o <i>procedural accountability</i> (Binns, 2018). Um modelo de responsabilização que enfatiza os processos através dos quais decisões algorítmicas são tomadas, em vez de apenas os resultados, promovendo documentação, explicabilidade e contestabilidade.
Capacitação institucional	Formação crítica e continuada dos profissionais, de modo a reforçar literacia tecnológica e capacidade de atuação ética e informada.
Dispositivos de escrutínio externo	Criação de conselhos independentes de avaliação e auditoria de tecnologias policiais, com competências para deliberar e sancionar, alinhados com boas práticas internacionais.
Infraestruturas digitais democráticas	Promoção de soluções tecnológicas de base pública, abertas à deliberação, adaptáveis às especificidades dos contextos locais e compatíveis com os direitos fundamentais.

Fonte: Autora (elaboração própria)

Nota(s) Conclusiva(s)

Este capítulo procurou contribuir para uma compreensão crítica das infraestruturas digitais no policiamento, a partir de uma perspetiva sociotécnica centrada nos contextos institucionais, discursos performativos e práticas quotidianas. A análise do caso português permitiu mostrar que os sistemas baseados em *Big Data* não apenas alteram rotinas operacionais, mas também reconfiguram as lógicas de governação, responsabilidade e visibilidade institucional.

As três dimensões exploradas — expectativas performativas, fragmentação da responsabilização e transparência seletiva — revelam que a opacidade tecnológica funciona como elemento estruturante, e não como mero efeito colateral. A promessa de inovação é frequentemente mobilizada como discurso de legitimidade, dissociando-se da prática concreta e dificultando a responsabilização. No entanto, as entrevistas também revelam formas de agência dos profissionais, que adaptam, contornam ou resistem às tecnologias, demonstrando que a digitalização policial é um processo em disputa, marcado por tensões e ambiguidades.

Neste contexto, é fundamental que as políticas públicas e os mecanismos regulatórios considerem não apenas os aspetos técnicos, mas também os impactos organizacionais e políticos destas tecnologias. A governação democrática exige dispositivos de escrutínio independente e espaços de deliberação que incluam todos os atores implicados — dos programadores à sociedade civil. Reforça-se ainda a importância de aprofundar a investigação empírica com abordagens comparativas, estudos interinstitucionais e análises dos impactos sobre os públicos afetados. Estes desenvolvimentos são cruciais para evitar que a inovação tecnológica legitime novas formas de exclusão e desresponsabilização.

Pensar as infraestruturas digitais policiais não é apenas uma questão técnica ou institucional, mas uma oportunidade crítica de imaginar outros modelos de segurança e participação democrática. Reconhecer que a tecnologia nunca é neutra é o primeiro passo para garantir que ela seja desenhada com e para os cidadãos.

Referências

- Amoore, L. (2020). *Cloud ethics: Algorithms and the attributes of ourselves and others*. Duke University Press.
- Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3), 973–989. <https://doi.org/10.1177/1461444816676645>
- Assembleia da República (2019, 8 de agosto). *Lei n.º 58/2019* [Diploma que assegura a execução do Regulamento (UE) 2016/679 (RGPD)]. *Diário da República*, 1.ª série, n.º 151. Disponível em <https://dre.pt/web/guest/pesquisa/-/search/123815982/details/normal>
- Babuta, A. (2017). Big Data and policing an assessment of law enforcement requirements, expectations and priorities. *Royal United Services Institute for Defence and Security Studies for Defence and Security Studies*, 1–41.
- Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), 855–881. <https://doi.org/10.1177/01622439211030007>
- Bietti, E. (2021). From ethics washing to ethics bashing: A moral philosophy view on tech ethics. *Journal of Social Computing*, 2(3), 266–283. <http://doi.org/10.23919/JSC.2021.0031>
- Bijker, W. E., & Law, J. (Eds.). (1992). *Shaping Technology/Building Society: Studies in Sociotechnical Change*. MIT Press.
- Borup, M., Brown, N., Konrad, K., & Van Lente, H. (2006). The sociology of expectations in science and technology. *Technology Analysis & Strategic Management*, 18(3–4), 285–298. <https://doi.org/10.1080/09537320600777002>
- Brayne, S. (2017). Big Data surveillance: The case of policing. *American Sociological Review*, 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.
- Clarke, A. E. (2005). *Situational analysis: Grounded theory after the postmodern turn*. Sage.
- Coglianesse, C., & Lehr, D. (2019). Transparency and algorithmic governance. *Administrative Law Review*, 71(1), 1–56.
- Comissão Europeia. (2023). *Relatório de 2023 Sobre o Estado da Década Digital*. <https://doi.org/10.2759/999709>
- Dempsey, R., Brunet, J., & Dubljević, V. (2023). Exploring and understanding law enforcement's relationship with technology: A qualitative interview study of police officers in North Carolina. *Applied Sciences*, 13(6), 1–17. <https://doi.org/10.3390/app13063887>
- Durão, S. (2008). Vigilância e controlo policiais: Precisões etnográficas. In C. Frois (Ed.). *A Sociedade Vigilante: Ensaio Sobre Privacidade, Identificação e Vigilância* (pp. 193–223). Lisboa: Imprensa de Ciências Sociais.
- Ferguson, A. (2018). Illuminating black data policing. *Ohio State Journal of Criminal Law*, 15(503), 503–525.
- Frois, C. (2013). *Peripheral Vision. Politics, Technology and Surveillance*. New York and Oxford: Berghahn Books.
- Geels, F., & Smit, W. (2000). Lessons from failed technology futures: Potholes in the road to the future. In N. Brown, B. Rappert, & A. Webster (Eds.), *Contested Futures: A Sociology of Prospective Techno-Science* (pp. 129–155). Farnham: Ashgate.
- Green, B. (2021). The contestation of tech ethics: A sociotechnical approach to technology ethics in practice. *Journal of Social Computing*, 2(3), 209–225. <https://doi.org/10.23919/JSC.2021.0018>
- 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>
- Jasanoff, S. (2004). *States of knowledge: The co-production of science and social order*. Routledge.
- Jones, T. (2012). The accountability of policing. In T. Newburn (Ed.), *Handbook of Policing* (pp. 721–752). Cullompton: Willan Publishing.

- Konrad, K. (2006). The social dynamics of expectations: The interaction of collective and actor-specific expectations on electronic commerce and interactive television. *Technology Analysis & Strategic Management*, 18(3-4), 429-444. <https://doi.org/10.1080/09537320600777192>
- Kinchin, N. (2024). "Voiceless": the procedural gap in algorithmic justice. *International Journal of Law and Information Technology*, 32(1), eaae024. <https://doi.org/10.1093/ijlit/eaae024>
- Kubler, K. (2017). State of urgency: Surveillance, power, and algorithms in France's state of emergency. *Big Data & Society*, 4(2), 1-10. <https://doi.org/10.1177/2053951717736338>
- Latour, B. (2010). Prendre le pli des Techniques. *Réseaux*, 163(5), 11-31.
- (1992). Where are the missing masses? The sociology of a few mundane artifacts. In Bijker, W. E., & Law, J. (Eds.), *Shaping Technology/Building Society*. MIT Press.
- (1987). *Science in action: How to follow scientists and engineers through society*. Harvard University Press.
- Law, J. (2008). On sociology and STS. *Sociological Review*, 56(4), 623-649. <https://doi.org/10.1111/j.1467-954X.2008.00808.x>
- (1991). *A Sociology of Monsters. Essays on Power, Technology and Domination*. New York and London: Routledge.
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.
- (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Machado, H., & Frois, C. (2014). Aspiring to modernization: Historical evolution and current trends of state surveillance in Portugal 1. In K. Boersma, R. Brake, C. Fonio et al. (Eds.), *Histories of State surveillance in Europe and beyond* (pp. 65-78). Routledge.
- Machado, H., & Silva, S. (2024). Risco e ética na governação da inteligência artificial: para além do ideário da União Europeia. In P. Urze, & E. Araújo (Eds.), *Estudos Sociais de Ciência e Tecnologia. Olhares e Perspetivas* (pp. 23-44). Lisboa: Tinta da China.
- Miranda, D. (2019). Identifying suspicious bodies? Historically tracing criminal identification technologies in Portugal. *Surveillance & Society*, 1-22. <https://doi.org/10.24908/ss.v18i1.12543>
- Monteiro, E., & Hanseth, O. (1996). Social shaping of information infrastructure: on being specific about the technology. In *Information Technology and Changes in Organizational Work: Proceedings of the IFIP WG8. 2 working conference on information technology and changes in organizational work, December 1995* (pp. 325-343). Springer US.
- Morgado, S., Felgueiras, S., & Moura, R. (2024). The past, present and future of technology in PSP: Preliminary results. In R. Fernandes, P. Machado, & L. Almeida (Eds.), *40 anos de Ciências Policiais em Portugal* (pp. 389-401). Lisboa: ICPOL — Centro de Investigação FCT do Instituto Superior de Ciências Policiais e Segurança Interna.
- Morgado, S., & Felgueiras, S. (2021). Big Data in policing: Profiling, patterns, and out of the box thinking. In Á. Rocha, H. Adeli, G. Dzemyda, F. Moreira, & A. Ramalho Correia (Eds.), *Trends and Applications in Information Systems and Technologies WorldCIST 2021. Advances in Intelligent Systems and Computing* (pp. 217-226). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-72657-7_21
- Neiva, L., & Machado, H. (2022). Rumo a uma implementação transparente, ética e inclusiva das tecnologias — o caso de Big Data na investigação criminal. In J. Sarmento & E. Araújo (Eds.), *Viagem e Cosmopolitismo: Da Ilha ao Mundo* (pp. 119-136). Vila Nova de Famalicão: Húmus.
- Neiva, L. (2024). *Expectativas de agentes policiais sobre Big Data no sistema de policiamento e investigação criminal em Portugal* [Tese de doutoramento, Universidade do Minho]. RepositórioUM.
- (2023). Big Data technologies in criminal investigations: The frames of the members of Judiciary Police in Portugal. *Criminology & Criminal Justice*, 1-23. <https://doi.org/10.1177/17488958231192767>
- Neiva, L., Machado, H., & Silva, S. (2023). The views about Big Data among professionals of police forces: A scoping review of empirical studies. *International Journal of Police Science & Management*, 25(2), 208-220.
- Nunes, J., & Gonçalves, M. (2001). Introdução. In J. Nunes & M. Gonçalves (Eds.), *Enteados de Galileu? A Semiperiferia no Sistema Mundial da Ciência* (pp. 13-31). Porto: Edições Afrontamento.

- Oatley, G. C. (2022). Themes in data mining, Big Data, and crime analytics. *WIREs Data Mining and Knowledge Discovery*, 12(2), e1432. <https://doi.org/10.1002/widm.1432>
- Oomen, J., Hoffman, J., & Hajer, M. A. (2022). Techniques of futuring: On how imagined futures become socially performative. *European Journal of Social Theory*, 25(2), 252–270. <https://doi.org/10.1177/1368431020988826>
- Ozili, P. K. (2025). Digital Public Infrastructure: Concepts, Global Efforts, Benefits, Challenges, and Success Stories. *Digital Society*, 4(30), 1–22. <https://doi.org/10.1007/s44206-025-00185-8>
- Pasquale, F. (2015). *The Black Box Society: The secret algorithms that control money and information*. Harvard University Press.
- Pereira, M. (2019). Big Data: o caso do sistema estratégico de informação, gestão e controlo operacional da Polícia de Segurança Pública [Dissertação de mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. <https://comum.rcaap.pt/handle/10400.26/30342>
- Philp, M. (2009). Delimiting democratic accountability. *Political studies*, 57(1), 28–53. <https://doi.org/10.1111/j.1467-9248.2008.00720.x>
- Pickering, A. (1992). *Science as Practice and Culture*. Chicago: University of Chicago Press.
- Rowe, M., & Muir, R. (2021). Big Data policing — Governing the machines? In J. McDaniel, & K. Pease (Eds.), *Predictive Policing and Artificial Intelligence* (pp. 254–269). Oxon and New York: Routledge.
- Sánchez-Monedero, J., & Dencik, L. (2022). The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl. *Information, Communication & Society*, 25(3), 413–430. <https://doi.org/10.1080/1369118X.2020.1792530>
- Schiölin, K. (2020). Revolutionary dreams: Future essentialism and the sociotechnical imaginary of the fourth industrial revolution in Denmark. *Social Studies of Science*, 50(4), 542–566. <https://doi.org/10.1177/0306312719867768>
- Schuppli, S. (2014). Deadly algorithms: Can legal codes hold software accountable for code that kills? *Radical Philosophy*, 191, 2–8.
- Silva, B. (2022). *Modernização da administração pública e os modelos de governação* [Dissertação de mestrado, Universidade de Coimbra].
- Sovacool, B., Bergman, N., Hopkins, D., Jenkins, K., Hielscher, S., Goldthau, A., & Brossmann, B. (2020). Imagining sustainable energy and mobility transitions: Valence, temporality, and radicalism in 38 visions of a low-carbon future. *Social Studies of Science*, 50(4), 642–679. <https://doi.org/10.1177/0306312720915283>
- Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, 7(1), 111–134. <https://doi.org/10.1287/isre.7.1.111>
- União Europeia (2016, 27 de abril). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados)*. *Jornal Oficial da União Europeia*, L 119, 1–88. Disponível em <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>
- União Europeia. (s.d.). *Horizonte 2020: O programa-quadro de investigação e inovação (2014–2020)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:horizon_2020
- Van Brakel, R. (2016). Pre-emptive big data surveillance and its (dis) empowering consequences: The case of predictive policing. In Exploring the Boundaries of Big Data. In B. van der Sloot, D. Broeders, & Erik Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 117–144). The Netherlands Scientific Council for Government Policy.
- Van Brakel, R., & Govaerts, L. (2024). Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society. *Theoretical Criminology*. <https://doi.org/10.1177/13624806241246267>
- Veale, M., Van Kleek, M., & Binns, R. (2018, April). Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. In *Proceedings of the 2018 chi conference on human factors in computing systems* (pp. 1–14).

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
<https://doi.org/10.1080/10439463.2023.2241965>

Wessels, M. (2024). Algorithmic policing accountability: eight sociotechnical challenges. *Policing and Society*, 34(3), 124-138. <https://doi.org/10.1080/10439463.2023.2241965>

Yin, R. (2011). *Qualitative Research from Start to Finish*. New York: Guildford Press.

Agradecimento

A autora expressa, em primeiro lugar, a sua gratidão à Polícia Judiciária e à Polícia de Segurança Pública, pela disponibilidade e interesse em participar na investigação que deu origem a este trabalho. Em segundo lugar, Laura Neiva agradece à Professora Doutora Helena Machado, pela inspiração e valioso feedback ao longo do percurso que originou este capítulo, bem como, à rede de investigação AIDA — social sciences research network (artificial intelligence, data & algorithms) pelos debates produtivos e inspiradores que estiveram na origem deste capítulo.

Financiamento

Este trabalho foi financiado pela FCT — Fundação para a Ciência e Tecnologia, I.P., — através da concessão de uma bolsa de doutoramento (referência 2020.04764.BD e DOI 10.54499/2020.04764.BD) com proveniência no orçamento nacional e no orçamento comunitário através do Fundo Social Europeu (FSE), e do projeto UIDB/00736/2020 (financiamento base) e UIDP/00736/2020 (financiamento programático). Este trabalho é financiado por fundos nacionais através da FCT — Fundação para a Ciência e a Tecnologia, I.P., no âmbito do Projeto <UID/04053/2025> com o identificador DOI <10.54499/UID/04053/2025> (<https://doi.org/10.54499/UID/04053/2025>) Este trabalho é financiado por fundos nacionais através da FCT — Fundação para a Ciência e a Tecnologia, I.P., no âmbito do financiamento UID/00736/2025: Centro de Estudos de Comunicação e Sociedade.

Nota biográfica

Laura Neiva é Professora Auxiliar na Universidade Lusíada — Porto e Professora Auxiliar convidada na Universidade do Minho, onde leciona nos cursos de Criminologia, Sociologia e no Mestrado em Crime, Diferença e Desigualdade. É investigadora júnior no Centro de Estudos Jurídicos, Económicos e Ambientais (Universidade Lusíada) e no Centro de Estudos de Comunicação e Sociedade (CECS-UMinho), bem como investigadora colaboradora no projeto fAIces (ERC Advanced Grant 101140664). Doutorada em Sociologia pela Universidade do Minho, desenvolveu investigação financiada pela FCT sobre as expectativas de agentes policiais acerca do Big Data no policiamento e na investigação criminal em Portugal. A sua investigação combina Criminologia, Sociologia e Estudos Sociais da Ciência e Tecnologia, centrando-se nos impactos éticos, políticos e sociais das tecnologias digitais. É autora do livro "Big Data na investigação criminal: desafios e expectativas na União Europeia" e de várias publicações sobre vigilância, políticas de segurança e inteligência artificial.

ORCID ID: [0000-0002-1954-7597](https://orcid.org/0000-0002-1954-7597)

CIÊNCIA ID: [A114-B97B-B443](https://ciencia.id/A114-B97B-B443)

Morada institucional: Universidade Lusíada Porto, Centro Universitário Lusíada Norte, Campus do Porto, Rua de Moçambique 21 e 71 (Aldoar), 4100-348 Porto, Portugal