Revista Lusófona de Estudos Culturais / Lusophone Journal of Cultural Studies, Vol. 12, N.º 1, 2025, e025002
https://doi.org/10.21814/rlec.6294

Entre os (Muitos) Sentidos de *Big Data*: A História, a Vigilância, o Controlo e a Criminalização

Laura Neiva
Centro de Estudos de Comunicação e Sociedade, Instituto de Ciências Sociais, Universidade do Minho, Braga, Portugal/Centro de Estudos Jurídicos, Económicos e Ambientais, Universidade Lusíada Norte, Porto, Portugal

Resumo

Este artigo analisa criticamente a vigilância na era de *big data*, explorando os múltiplos sentidos que lhe são atribuídos ao longo do tempo e traçando um mapeamento histórico da sua evolução. Sustentado nos estudos da vigilância, examina como estas práticas foram moldadas por dinâmicas sociotécnicas e securitárias, desde os seus primórdios associados à gestão populacional e ao policiamento, até à consolidação de infraestruturas algorítmicas baseadas na datificação massiva. Ao longo desta trajetória, argumenta-se que, longe de representar uma rutura absoluta, *big data* reconfigura e amplia mecanismos históricos de controlo, promovendo a fusão entre vigilância em massa e vigilância direcionada. A análise desenvolvida evidencia como as tecnologias de monitorização se inscrevem em narrativas tecno-otimistas que legitimam a sua expansão, enquanto reforçam a coletivização da suspeição e deslocam a lógica da investigação criminal para um modelo preditivo e estatístico. Através do estudo sumário do caso português, discute-se como a adoção de tecnologias reflete uma vontade política de modernização securitária, enquadrada por discursos que apresentam a tecnologia como solução incontornável para a criminalidade. Conclui-se que a vigilância algorítmica não só reestrutura o policiamento e a justiça criminal, mas também levanta desafios éticos e políticos significativos. A crescente opacidade dos processos de decisão automatizados e a sua naturalização no discurso securitário impõem a necessidade de um escrutínio crítico, de modo a evitar que a eficiência tecnológica se torne um princípio incontestado de governação, comprometendo direitos fundamentais e reproduzindo desigualdades estruturais.

Palavras-chave

vigilância, *big data*, polícia, segurança, história

Among the (Many) Meanings of Big Data: History, Surveillance, Control, and Criminalisation

Abstract

This article critically analyses surveillance in the era of big data, exploring the multiple meanings attributed to it over time and tracing its historical evolution. Drawing on surveillance studies, it examines how surveillance practices have been shaped by socio-technical and security dynamics — ranging from early efforts focused on population management and policing to the consolidation of algorithmic infrastructures grounded in mass datafication. Rather than representing a definitive rupture, big data is shown to reconfigure and expand historical mechanisms of control, fostering a convergence between mass and targeted surveillance.

The analysis demonstrates how monitoring technologies are embedded in techno-optimistic narratives that legitimise their proliferation while simultaneously reinforcing the collectivisation of suspicion and reorienting criminal investigation towards predictive and statistical models. Through a brief examination of the Portuguese context, the article discusses how the adoption of such technologies reflects a political aspiration for security modernisation, framed by discourses that portray technology as an inevitable response to crime. It concludes that algorithmic surveillance not only restructures policing and criminal justice but also raises profound ethical and political concerns. The increasing opacity of automated decision-making and its naturalisation within security discourse underscores the need for critical scrutiny to ensure that technological efficiency does not become an unquestioned principle of governance — at the expense of fundamental rights and the reproduction of structural inequalities.

Keywords
surveillance, big data, police, security, history

1. Introdução

Big data, entendida como um conjunto de ferramentas concebidas para processar e analisar grandes volumes de dados heterogéneos, identificando correlações e padrões, tem sido amplamente promovida como uma solução eficaz para a tomada de decisão em múltiplas esferas da vida social. No domínio da segurança pública e da investigação criminal, estas tecnologias são frequentemente legitimadas através de narrativas tecno-otimistas, que enfatizam a sua capacidade de reforçar a eficiência policial e a gestão do risco. No entanto, uma análise histórica da vigilância demonstra que a expansão destas infraestruturas não representa uma rutura, mas sim a adaptação e ampliação de práticas securitárias preexistentes, que consolidam lógicas de controlo e criminalização diferencial.

Este artigo propõe-se a traçar um mapeamento histórico da vigilância e das tecnologias associadas, analisando como o seu desenvolvimento moldou e foi moldado por contextos sociais, políticos e económicos. Partindo do conceito de "capitalismo dos dados" (Lyon, 2019), argumenta-se que a crescente centralidade da vigilância algorítmica reflete dinâmicas históricas de poder, promovendo a fusão entre vigilância em massa e vigilância direcionada, ao mesmo tempo que intensifica a coletivização da suspeição e redefine os contornos da segurança pública.

Para tal, inspira-se no trabalho do sociólogo David Lyon (2014a), especialista em estudos da vigilância, para compreender como os múltiplos sentidos da vigilância foram sendo reconfigurados ao longo do tempo. Como o próprio Lyon (2014a) salienta, "as tecnologias de hoje nascem de ontem" e, por isso, "um sentido de história é extremamente necessário para compreender o contexto do contemporâneo" (p. 33). Através desta perspetiva, este artigo procura densificar a compreensão da emergência de *big data*, analisando o seu papel na vigilância contemporânea e as suas implicações sociais, particularmente no que diz respeito à transição do policiamento reativo para modelos preditivos baseados em algoritmos.

Neste contexto, discute-se ainda a incorporação dessas tecnologias no panorama securitário português, demonstrando como a adoção de tecnologias reflete tanto uma estratégia de modernização como um alinhamento com discursos globais sobre a inevitabilidade tecnológica. Assim, ao longo deste artigo, argumenta-se que a vigilância algorítmica não apenas reconfigura as fronteiras entre segurança e controlo social, mas também impõe desafios éticos e políticos que exigem um escrutínio crítico sobre as suas promessas, limitações e riscos.

2. A(s) Trajetória(s) Histórica(s) da Vigilância e de *Big Data*: Do Controlo Estatal à Dataficação Algorítmica

Uma análise da evolução da vigilância ao longo das últimas três décadas permite delinear dois grandes eixos de desenvolvimento que moldam tanto o presente quanto as projeções futuras de *big data*. Por um lado, verifica-se a expansão da vigilância estatal, historicamente orientada para a recolha, processamento e análise de dados populacionais com o propósito de monitorizar, regular e influenciar comportamentos sociais e políticos (Haggerty & Ericson, 2007; Lyon, 2001a). Por outro lado, assiste-se ao avanço de novas tecnologias digitais que viabilizam a materialização dessa vigilância de forma cada vez mais sofisticada, recorrendo a sensores inteligentes, algoritmos preditivos e técnicas de *data mining*[1] para produzir inteligência estratégica (Gandy, 2006).

Este processo de inovação técnico-científica conduziu ao que Corbett e Marx (1991) denominaram de "nova vigilância", marcada pela integração de dispositivos digitais, biométricos e preditivos no campo securitário. Tais desenvolvimentos foram amplificados pelo combate ao terrorismo e aos crimes transfronteiriços (Bigo, 2006), adquirindo legitimidade política e institucional. Os atentados de 2001 nos Estados Unidos da América e, subsequentemente, os ataques em Madrid (2004), Londres (2005), Paris (2015) e Bruxelas (2016) impulsionaram a adoção massiva dessas tecnologias, promovendo um entusiasmo crescente em torno das suas promessas de eficiência na identificação de indivíduos e na prevenção de ameaças criminais (Beck, 2002; Bunyan, 2010; Monahan, 2010; Monar, 2008).

A resposta securitária global a essas ameaças incentivou uma maior cooperação policial e judiciária transnacional, consolidando a vigilância digital como um pilar central das políticas de segurança pública. Contudo, é essencial evitar o que Corbett e Marx (1991) classificam como "a falácia das agendas explícitas" (p. 402) — a ilusão de que estas tecnologias emergem com propósitos exclusivamente técnicos, livres de interesses políticos ou estruturais. Como assinala Lyon (2015), a recolha massiva de dados e o uso de ferramentas analíticas avançadas não são apenas subprodutos do progresso tecnológico, mas refletem abordagens estratégicas de gestão do risco em indústrias securitárias, onde populações inteiras passam a ser classificadas estatisticamente, independentemente da existência de suspeitas concretas (Norris & McCahill, 2006).

[1] Processo informático com o objetivo de encontrar anomalias, padrões e correlações entre conjuntos de dados para prever resultados (Pramanik et al., 2017).

Esta vigilância orienta-se não apenas para indivíduos identificados, mas também para categorias de pessoas, redes, espaços geográficos ou temporais considerados de risco (Marx, 2002), marcando uma inovação significativa face à vigilância tradicional.

A crescente legitimação pública e política das redes de vigilância tem levado à proliferação de sistemas interconectados, concebidos para identificar, classificar e controlar indivíduos e grupos. Exemplos paradigmáticos incluem o *European Dactyloscopy*, criado em 2003 para a comparação de impressões digitais de requerentes de asilo; o *Visa Information System*, operacional desde 2011, que permite a partilha de dados sobre vistos entre os Estados-membros da área Schengen; e as Decisões Prüm (Decisão 2008/615/JAI, 2008; Decisão 2008/616/JAI, 2008), que regulam a troca de dados genéticos, registos de veículos e impressões digitais como estratégia de combate ao terrorismo e ao crime organizado.

Este panorama de vigilância integrada foi amplificado pela convergência de sistemas dispersos numa complexa *assemblage* de vigilância (Deleuze & Guattari, 1987; Haggerty & Ericson, 2007; Lyon, 2022), caracterizada pela abstração dos corpos físicos e pela sua reconfiguração como fluxos de dados invisíveis (Haggerty & Ericson, 2000). A datificação das sociedades (Cukier & Mayer-Schoenberger, 2013) transformou os indivíduos em entidades estatísticas, com implicações profundas no modo como são categorizados, monitorizados e controlados. Como enfatiza Strauß (2018), este processo de reconfiguração digital resulta na fragmentação dos sujeitos em "pontos de dados" (p. 56), redefinindo os limiares da vigilância contemporânea.

A ascensão de *big data* intensificou a *dataveillance* (Clarke, 1988; Garfinkel, 2000; Lyon, 2022), ou seja, a monitorização sistemática de ações e interações através de vastos sistemas de recolha e processamento de dados. Esta tendência consolidou um ecossistema onde a monitorização de padrões e a categorização algorítmica não apenas orientam a regulação do comportamento individual, mas também fomentam uma lógica de mercado assente na exploração comercial da informação pessoal — o capitalismo dos dados (Zuboff, 2019). Como evidenciado por Esposti (2014), esta vigilância digitalizada não se limita ao contexto securitário, expandindo-se para a economia de dados, onde a segmentação de perfis e a predição de tendências comportamentais servem interesses empresariais e políticos.

Deste modo, a vigilância e o controlo do crime passaram a estar indissociavelmente ligados à constituição das subjetividades modernas, operando através da mediação de fluxos de informação que transitam entre computadores, bases de dados e redes interconectadas (Machado, 2021). Nos Estados Unidos da América, a massificação da vigilância estendeu-se para além das instituições tradicionalmente responsáveis pelo controlo criminal, abrangendo setores como a saúde e a educação, dando origem ao que Garland (2001) classifica como uma sociedade de controlo. Esta lógica de monitorização permanente, outrora restrita a contextos específicos de policiamento, foi gradualmente globalizada, convertendo-se numa infraestrutura sociotécnica essencial às dinâmicas contemporâneas de governança. Como sublinhado por Lyon (1994, 2001a), este processo culmina na transição para uma sociedade caracterizada por vigilância contínua, marcada

por estados de vigilância máxima (Corbett & Marx, 1991; Norris & Armstrong, 1999), onde a distinção entre segurança e controlo se torna cada vez mais difusa.

O mapeamento desta(s) trajetória(s) permite compreender o modo como a evolução da vigilância e de *big data* não é um processo neutro ou meramente técnico, mas sim uma manifestação de transformações estruturais que redefinem as fronteiras entre o público e o privado, o visível e o invisível, o permitido e o proibido. A datificação da sociedade não apenas ampliou os mecanismos de observação e regulação, mas também deslocou os processos de decisão para sistemas algorítmicos que operam com opacidade crescente. Mais do que substituir a tomada de decisão, essas tecnologias procuram, inclusivamente — e talvez de modo mais insidioso — moldar ou determinar decisões ao nível individual, condicionando escolhas, comportamentos e trajetórias de vida de forma impercetível e contínua (Zuboff, 2019). Assim, compreender a vigilância contemporânea exige um olhar atento às suas raízes históricas, às suas continuidades e ruturas e, sobretudo, às suas implicações no delineamento das sociedades futuras.

3. A Vigilância na Era de *Big Data*: Expansão das Redes, Gestão do Risco e Novas Tecnologias

As transformações contemporâneas da vigilância refletem uma transição paradigmática das práticas disciplinares para estratégias securitárias baseadas na gestão do risco (Cunha, 2008; Maciel & Machado, 2014). Este deslocamento traduz uma mudança de enfoque: de um modelo voltado para a erradicação do crime por meio da disciplina, para um modelo que privilegia a previsão do crime, estruturando as políticas securitárias em torno da identificação e minimização de riscos (Garland, 2001; Lyon, 2004). Neste contexto, as novas tecnologias e técnicas de vigilância passaram a ser promovidas sob a promessa de maior eficiência na manutenção da segurança (Bygrave, 2002; Lyon, 2001b), legitimando um investimento crescente na sua implementação.

As tabelas que Foucault (1975/1999) identificava como instrumentos fundamentais do poder disciplinar no século XVIII foram transmutadas, na atualidade, em vastas bases de dados digitais, eliminando a necessidade de mecanismos disciplinares físicos e visíveis. A vigilância contemporânea, ao expandir-se da disciplina para a segurança (Cunha, 2008), para o controlo (Deleuze & Guattari, 1987) e para a gestão do risco (de Laat, 2019), consolidou-se enquanto tecnologia de poder, sendo amplamente financiada, elogiada e defendida pelo seu valor simbólico e funcional na regulação social (Baird, 2018; Monahan, 2010). Esta valorização possibilitou investimentos substanciais em infraestruturas destinadas à identificação, monitorização e análise de dados individuais (Monahan, 2010).

Com a sua crescente expansão, empresas privadas especializadas em segurança passaram a integrar algoritmos avançados para cruzar dados provenientes de diversas fontes, como registos bancários, médicos e *cookies* de navegação na internet (Lyon, 2015; Miller, 2014). Este processo resultou na integração das bases de dados como uma ferramenta essencial na atuação policial (Durão, 2009; Ericson & Haggerty, 1997; Van Brakel & De Hert, 2011), permitindo a centralização, armazenamento e processamento massivo

de informações sobre suspeitos e condenados (Durão, 2009; Haggerty, 2012; Van Brakel & De Hert, 2011). Por exemplo, assiste-se à substituição progressiva dos arquivos físicos e da recolha presencial de informações (Marx, 1988) por sistemas de vigilância em massa de natureza quotidiana (Ball & Webster, 2003), onde a quantificação do perigo (Machado & Santos, 2016) passa a orientar intervenções preditivas no policiamento.

Embora frequentemente tratadas como inovações recentes, as práticas de quantificação do risco e predição da criminalidade remontam a períodos históricos anteriores. McQuade (2021) salienta que "uma perspetiva histórica mais longa sugere que esta mudança contemporânea no policiamento pode ser mais cíclica do que singular, um regresso a um momento anterior e não uma rutura definitiva com o passado" (p. 113), reforçando a continuidade histórica entre os modelos preditivos atuais e abordagens anteriores à gestão do crime. Exemplos dessa continuidade incluem, em 1925, a Escola de Chicago (Park & Burgess, 1925), que introduziu um modelo probabilístico para prever a reincidência criminal no âmbito da liberdade condicional. Durante as décadas de 1970 e 1980, os tribunais dos Estados Unidos da América implementaram a quantificação de dados como critério de decisão (Afzal & Panagiotopoulos, 2024), consolidando abordagens atuariais que utilizam indicadores numéricos para gerir o risco criminal (McCahill, 2022; Neiva, 2020). Em 1994, o programa CompStat foi desenvolvido em Nova Iorque como um sistema de análise de padrões criminais para orientar a alocação de recursos policiais (Afzal & Panagiotopoulos, 2024; Creemers, 2021).

A incorporação destas abordagens no sistema de justiça criminal impulsionou o crescimento do policiamento preditivo, baseado na análise estatística para a identificação de tendências criminais futuras (Amoore, 2011; Lyon, 2004). Como resultado, reemerge o que Feeley e Simon (1992) denominam de "justiça atuarial" ou "nova penologia", caracterizada pelo uso de dados para avaliar riscos individuais e coletivos. Esta transição foi acompanhada pelo desenvolvimento de tecnologias de inteligência que permitem a classificação e monitorização de indivíduos em larga escala, utilizando a informação analisada para fundamentar estratégias de controlo social (Garland, 2001; Innes et al., 2005; Kirby & Keay, 2021; Newburn, 2012). A integração destas tecnologias criou novos paradigmas de vigilância, caracterizados pela ausência de barreiras físicas e pela invisibilidade dos processos de monitorização. Como observou Poster (1990) há 35 anos atrás — e a sua reflexão continua atual —, "sistemas de vigilância sem paredes, janelas, torres ou guardas" (p. 93) tornaram-se a norma, eliminando a necessidade de contacto físico direto com os indivíduos sob vigilância (Marx, 2006).

Nesta lógica, a vigilância contemporânea incorpora os princípios do biopoder conceptualizados por Foucault (2003), operando não apenas sobre corpos individuais, mas sobre populações inteiras (Ericson & Haggerty, 1997). A categorização de indivíduos segundo critérios de risco reflete a racionalidade do biopoder, que procura gerir fluxos sociais através da separação entre a "boa" e a "má" circulação (Foucault, 2008, p. 34). *Big data* é, assim, um exemplo paradigmático de uma tecnologia de gestão securitária, onde o controlo da criminalidade passa pela segmentação populacional e pela quantificação estatística da ameaça, legitimando intervenções policiais orientadas por perfis de risco.

O uso de algoritmos para classificar e prever comportamentos futuros deu azo a um processo de segregação digital, onde zonas geográficas e grupos populacionais são sinalizados de acordo com índices de perigosidade atribuídos por modelos matemáticos (Duxbury & Andrabi, 2022; Graham, 2006). Simultaneamente, o policiamento preditivo e as avaliações de risco reforçam a normalização da vigilância algorítmica (Ericson & Haggerty, 1997; Feeley & Simon, 1992; Garland, 1997), tornando-a um mecanismo característico das sociedades contemporâneas.

Em termos práticos, esta transformação desloca o foco do sistema de justiça criminal: do estudo das causas do crime para a identificação de potenciais suspeitos (Andrejevic et al., 2020). Esta mudança implica que, ao invés de compreender os fatores estruturais que conduzem ao crime, a prioridade passa a ser a antecipação de que indivíduos ou grupos poderão cometer crimes no futuro. Como consequência, a análise massiva de dados populacionais substitui a investigação tradicional baseada em indícios concretos, ampliando o uso de avaliações preditivas no controlo social (Dencik, 2022). Exemplos desta abordagem incluem a ferramenta Harm Assessment Risk Tool, utilizada pela polícia de Durham no Reino Unido, que prevê a probabilidade de um indivíduo cometer um crime nos dois anos seguintes (Justice and Home Affairs Committee, 2022). Estas práticas inscrevem-se num modelo de vigilância sustentado na agregação massiva de dados, onde a categorização dos indivíduos em função do risco securitário se converte num princípio central.

Estas dinâmicas contemporâneas suscitam reflexões renovadas sobre o panótico inicialmente concebido por Jeremy Bentham no século XVIII[2] (Innes, 2003; Mathiesen, 1997). Embora criticado por autores como Bogard (1996, 2006) e Haggerty (2006), o panótico continua a oferecer uma lente interpretativa útil para compreender as reconfigurações da vigilância digital. No entanto, o seu modelo clássico foi substituído por um panótico tecnológico, caracterizado pela mobilidade e descentralização dos dispositivos de monitorização (Cunha, 2008), cuja omnipresença permeia a sociedade e expande os seus tentáculos para além dos espaços físicos delimitados (Corbett & Marx, 1991). *Big data*, neste contexto, emerge como a manifestação contemporânea desta lógica vigilante, consolidando-se enquanto a próxima geração de segurança (War Studies KLC, 2022), moldando práticas policiais, redefinindo fronteiras sociais e institucionalizando um *ethos* securitário ancorado na recolha e processamento de dados em larga escala.

[2] Uma estrutura arquitetónica no interior das prisões concebida para possibilitar um controlo contínuo e permanente da população reclusa, utilizando o espaço e a luz como mecanismos de vigilância (Bentham, 1995). Integrada num sistema disciplinar baseado numa vigilância hierárquica (Foucault, 1975/1999), esta configuração consistia numa torre central, rodeada por celas dispostas em anel, onde os guardas podiam observar os reclusos sem serem vistos. Essa assimetria visual fazia com que os reclusos interiorizassem a sensação de estarem constantemente sob vigilância, funcionando como um mecanismo de disciplina e autorregulação. Para além do contexto prisional, Foucault (1975/1999) expande estes princípios de controlo para a sociedade em geral, demonstrando como a lógica panótica se manifesta em diversas estruturas de poder e vigilância.

4. A Convergência da Vigilância Tradicional e de *Big Data*: Novos Paradigmas e Tensões Sociotécnicas

O advento de *big data* promove a interseção entre dois tipos de vigilância tradicionalmente distintos: a vigilância em massa e a vigilância direcionada. A primeira, conforme concebida por Lyon (2014b, 2015), pressupõe que qualquer indivíduo pode ser detetado no vasto ecossistema de vigilância, ao passo que a segunda visa a identificação e monitorização de suspeitos específicos. No entanto, com a expansão de *big data*, estas categorias tornam-se cada vez mais indistintas, levando a uma fusão metodológica e operacional (Brayne, 2014, 2022). Embora *big data* permita a recolha massiva de dados, opera, em última instância, sob uma lógica de vigilância direcionada, na medida em que a sua finalidade última é a identificação de sujeitos considerados suspeitos (Lyon, 2015). Neste quadro, Margaret Hu (2015) argumenta que estas tecnologias constroem um mundo de potenciais suspeitos, onde a recolha indiscriminada de dados sobre todos os cidadãos viabiliza a criação de associações digitais entre indivíduos e eventos criminais passados ou futuros (Hu, 2015; Van Brakel & Govaerts, 2024). Esta lógica expande a malha da vigilância (Joh, 2016), deslocando-se de um modelo baseado na monitorização de suspeitos previamente identificados para uma abordagem mais ampla, que integra toda a população sob um potencial escrutínio (Miranda, 2020). Neste quadro, o controlo deixa de incidir sobre eventos específicos e torna-se contínuo, ilimitado e modular, em consonância com o que Deleuze (2006) designou como as "sociedades de controlo" — contextos em que a suspeição já não é um estado transitório, mas uma condição latente e permanente.

Schafer et al. (2011) apontam que este novo ecossistema de segurança transforma a lógica tradicional da presunção de inocência — onde apenas alguns indivíduos são monitorizados — para um paradigma de presunção de culpa, no qual todos os cidadãos são sujeitos, pelo menos superficialmente, a escrutínio constante[3]. *Big data* torna possível a convergência destes dois modos de observação, associando representações digitais dos indivíduos à sua presença física (Hu, 2015), criando perfis baseados em projeções algorítmicas que influenciam a atuação policial (Blount, 2024). O objetivo já não é apenas investigar um indivíduo-alvo com base em suspeitas fundamentadas, mas sim antecipar e moldar o futuro, desenvolvendo modelos preditivos que, a partir de dados agregados, projetam cenários de risco e fundamentam estratégias de controlo social (Hu, 2015). Tal como descreve Latour (1987), a construção destes centros de cálculo — bases de dados e sistemas algorítmicos — permite a recolha e o processamento de informações dispersas, que são reconfiguradas à distância e transformadas em conhecimento operacional para instituições policiais e securitárias (Haggerty & Ericson, 2000). Assim, a vigilância de *big data* não apenas opera a partir de uma crescente abstração dos corpos físicos, mas também reforça um modelo de governação securitária baseado na gestão algorítmica do risco.

[3] Algumas bases de dados forenses exemplificam esta lógica, ao manterem perfis genéticos de indivíduos não condenados, apenas identificados, que passam a ser permanentemente rastreáveis em investigações futuras. Esta inscrição biométrica opera como um marcador de suspeição contínua, em que a presunção de inocência é progressivamente substituída por uma lógica de vigilância latente e automatizada (Kruse, 2010).

Apesar das aparentes distinções entre vigilância tradicional e vigilância baseada em *big data*, verifica-se um núcleo comum entre ambas: a monitorização e o controlo dos indivíduos. Se a vigilância tradicional se materializa através do patrulhamento e da observação direta, *big data* substitui essa proximidade física por um sistema digitalizado de monitorização e categorização, construindo uma distância simbólica no ato de vigiar, o que permite inferir padrões de comportamento e construir cenários futuros com base em dados previamente recolhidos (Lyon, 2022). Este fenómeno traduz-se num modelo de controlo à distância, operado por processos algorítmicos que transformam os indivíduos em representações numéricas, categorizando-os sob uma gramática digital despersonalizada (Frois, 2008). Como Brayne (2022) observa, a digitalização massiva da informação constitui "a principal tendência secular que molda a vigilância nas últimas décadas" (p. 372). Esta transformação configura um novo regime de monitorização que está cada vez mais imbricado em infraestruturas tecnológicas (Lyon, 2022). A proliferação dessas novas formas de vigilância estendeu-se a nível global e europeu, tornando-se uma componente estrutural dos sistemas de controlo social (Machado, 2021). O conhecimento produzido por análises computorizadas ganha progressivamente primazia sobre a experiência prática dos agentes policiais, criando tensões entre modelos de decisão baseados na ontologia algorítmica e aqueles sustentados por narrativas interpretativas tradicionais (Machado, 2021).

Este contexto permite compreender como *big data* se insere num modelo de governação tecnosecuritário, no qual a necessidade, a autoridade e a verdade são instrumentalizadas para legitimar a vigilância massiva (Skinner, 2018). A confiança inquestionável nas tecnologias, sustentada por um discurso de infalibilidade científica (Costa et al., 2002), contribui para a subjugação dos indivíduos, comprometendo direitos fundamentais como a liberdade, a igualdade, a presunção de inocência e a autodeterminação identitária (Blount, 2024; Sachoulidou, 2023). A disseminação de narrativas laudatórias sobre o papel das tecnologias digitais na segurança pública tem sido determinante para a aceitação social dessas práticas, inscrevendo na imaginação coletiva a ideia de que o poder das tecnologias é imprescindível para a prevenção do crime (ver, também, Prainsack & Toom, 2010) — um imaginário amplamente reforçado também por representações ficcionais populares, como *Person of Interest* (Sob Suspeita; Grondin & Hogue, 2024) ou *CSI — Criminal Scene Investigation* (Crime Sob Investigação; Machado & Santos, 2012; Schweitzer & Saks, 2007), que glorificam o uso de sistemas inteligentes de vigilância e investigação. Este imaginário securitário tem influenciado o desenvolvimento de infraestruturas de vigilância cada vez mais automatizadas. No Departamento de Polícia de Los Angeles, por exemplo, Brayne (2017) documenta que, desde 2015, os sistemas de consulta policial foram complementados por alertas automatizados: em vez de dependerem exclusivamente da pesquisa manual de informações por parte dos agentes, as bases de dados passaram a gerar notificações em tempo real sempre que os algoritmos detetam padrões considerados anómalos. Como refere Elizabeth Joh (2016), esta transformação representa "uma expansão importante nos poderes da polícia" (p. 16), pois amplia significativamente as suas capacidades operacionais (Volkwein, 2022) e aprofunda a interseção entre vigilância e exploração de *big data* (Rowe & Muir, 2021).

Neste cenário, as funções policiais sofrem uma mutação substancial, passando de uma lógica de repressão e punição para um modelo de controlo baseado na recolha, análise e gestão da informação (Ericson & Haggerty, 1997). Assim, a adoção de tecnologias de vigilância enquanto instrumentos estruturantes da ação policial reflete uma crença na infalibilidade da tecnologia, inscrevendo-se num *ethos* securitário que redefine a cultura penal e a administração da justiça na contemporaneidade (Machado, 2021). Por exemplo, discursos na Assembleia da República (Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, 2021) que sublinharam a aceitação da videovigilância como um instrumento útil na prevenção e combate ao crime, refletindo a confiança das autoridades na tecnologia para manter a ordem pública e a segurança; e em eventos policiais nacionais e internacionais, como o "AIDA Information Day" e o "VI Congresso de Investigação Criminal da Polícia Judiciária" em 2023, onde os participantes se referiam às valências e oportunidades trazidas por *big data* no contexto criminal, enfatizando que "vai diminuir o tempo da investigação", "irá capacitar as agências da lei com soluções promissoras", "há uma necessidade de tirar o maior proveito da tecnologia", "trata-se de um admirável mundo novo" e "traz oportunidades para a investigação criminal" (Neiva, 2024, p. 289).

5. A Modernização da Vigilância em Portugal: Entre a História, a Tecnologia e a Legitimação do Controlo

A evolução da vigilância em Portugal tem sido fortemente moldada pelos avanços tecnológicos e pela sua crescente incorporação nos sistemas de policiamento e investigação criminal. A trajetória nacional reflete uma passagem dos arquivos em papel e máquinas de escrever para sistemas digitais de armazenamento e processamento de dados policiais. Esta transição inclui, não apenas novos meios de comunicação e transporte, mas também a digitalização das metodologias de partilha de informação criminal, consolidando um processo contínuo de modernização e inovação tecnológica (Miranda, 2020). Desde a aplicação de metodologias antropométricas destinadas à caracterização de indivíduos com base nas suas características físicas e corporais até à criação de bases de dados forenses de impressões digitais e DNA, Portugal acompanhou, ainda que de forma intermitente, as transformações globais da vigilância (Machado & Frois, 2014). Neste contexto, a informatização dos sistemas policiais tornou-se um instrumento central, permitindo uma recolha, registo e partilha interna cada vez mais automatizada da informação criminal (Durão, 2009).

Apesar dessa aspiração modernizadora, a adoção de tecnologias de vigilância no país não ocorreu de forma linear ou isenta de obstáculos. Uma análise histórica revela como as descontinuidades entre o passado, o presente e o futuro da tecnologia condicionaram a implementação de inovações neste domínio. Entre os fatores mais determinantes encontra-se a ditadura de António de Oliveira Salazar (1926–1974), que inseriu Portugal num modelo político conservador, repressivo e avesso à inovação tecnológica. O regime do Estado Novo, sustentado por uma estrutura censória e um

forte aparelho de vigilância política, operado pela Polícia Internacional e de Defesa do Estado, recusava qualquer inovação que pudesse fragilizar os seus mecanismos de controlo e repressão (Pimentel, 2024).

A Revolução dos Cravos, em 1974, marcou a rutura com esse sistema autoritário, mas a modernização tecnológica das infraestruturas de vigilância e segurança pública não ocorreu de imediato. O grande impulso deu-se três décadas depois, com a organização do Campeonato Europeu de Futebol — Euro 2004[4]. A magnitude do evento exigiu um reforço significativo das infraestruturas de segurança, o que conduziu à adoção e expansão de tecnologias de monitorização em espaços públicos. Esta evolução alinha-se com processos observados noutros países, como a Grécia, onde a implementação de CCTV (*Closed-Circuit Television*) nos Jogos Olímpicos refletiu um modelo de segurança altamente tecnocrático, priorizando a supremacia tecnológica sobre estratégias tradicionais de policiamento (Frois & Machado, 2016).

A implementação de circuitos de videovigilância públicos em Portugal teve início em 2005, expandindo uma prática que até então era restrita a espaços fechados (Frois, 2014). Contudo, apesar do entusiasmo político em torno da sua adoção, a disseminação desta tecnologia encontrou resistência significativa. Em 2010, três locais possuíam sistemas de videovigilância autorizados e em funcionamento — Porto, Coimbra e o Santuário de Fátima —, e até 2012, dois sistemas permaneceram ativos devido aos entraves impostos pela autoridade de proteção de dados[5] (Machado & Frois, 2014).

O ano de 2005 também marcou o início de uma proposta de criação de uma base de dados genética nacional, com vocação universal, apresentada no programa do XVII Governo Constitucional. Esta base visava tanto a identificação civil como a investigação criminal. Sob o argumento da eficiência no combate ao crime, a base de dados foi concretizada e legislada em 2008[6]. O desenvolvimento deste projeto insere-se numa tendência europeia mais ampla de adoção de tecnologias forenses digitais, ilustrada, por exemplo, pela Recomendação n.º R (92) 1 (1992), do Conselho da Europa, sobre o uso de dados genéticos na justiça penal, e pelo Tratado de Prüm, que regulamenta a partilha de dados genéticos entre Estados-membros da União Europeia. Neste sentido, o caso português reflete uma dinâmica transnacional de alinhamento com políticas securitárias tecnológicas, nas quais o uso de tecnologias forenses sofisticadas é mobilizado como um instrumento de reforço do policiamento e da segurança pública.

---

[4] Embora, apenas dois anos após a Revolução de 25 de abril de 1974, já se observassem algumas mudanças, nomeadamente com a criação de um arquivo central de identificação civil e criminal, instituído pelo Decreto-Lei n.º 63/1976, de 24 de janeiro (Miranda, 2020).

[5] "A Comissão Nacional de Proteção de Dados (CNPD) é uma entidade administrativa independente (...) com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República. A CNPD controla e fiscaliza o cumprimento do Regulamento Geral de Proteção de Dados, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais." (Comissão Nacional de Proteção de Dados, s.d.).

[6] Lei n.º 5/2008, de 12 de fevereiro, que aprova a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal (Procuradoria-Geral Regional de Lisboa, s.d.).

Esta evolução das tecnologias de vigilância em Portugal deve ser compreendida, como argumentam Helena Machado e Catarina Frois (2014), no âmbito de uma "formulação de políticas no sentido mais amplo" (p. 75), que se insere numa ambição coletiva de modernização securitária. Esta narrativa modernizadora fundamenta-se num discurso político que apresenta a tecnologia como solução para o combate ao crime, atribuindo-lhe um papel central na construção de uma sociedade mais segura e eficiente (Frois, 2014; Miranda, 2020). Assim, tanto a implementação de sistemas de videovigilância como a criação da base de dados genéticos ilustram o desejo nacional de alinhamento com práticas consideradas tecnologicamente avançadas e, muitas vezes, guiado por uma imaginação do centro, na qual os modelos institucionais e técnicos de países centrais são tomados como referência incontornável de progresso e modernidade (Ribeiro, 2004). Neste caso, reforçando a crença de que estas ferramentas são mais eficazes do que os métodos tradicionais de investigação criminal.

Mais do que meros instrumentos de segurança, essas tecnologias tornam-se representações simbólicas da evolução do país e da sua capacidade de adaptação a padrões internacionais. Como observa Diana Miranda (2020), "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" (p. 6; ver também Frois, 2013; Nunes & Gonçalves, 2001). Deste modo, a adoção dessas tecnologias não responde apenas às necessidades securitárias concretas, mas também a um desejo de superação da condição periférica do país, evidenciando a tecnologia como um símbolo de progresso e sofisticação no campo da vigilância e do controlo social.

6. Conclusões

A análise aqui desenvolvida permitiu compreender como a vigilância e as tecnologias associadas à *big data* se têm consolidado como infraestruturas fundamentais do policiamento e da investigação criminal contemporânea. A evolução histórica das práticas de controlo evidencia uma trajetória marcada por (des)continuidades, onde antigos mecanismos de poder são reconfigurados e adaptados a novos contextos sociotécnicos. A vigilância, longe de ser um fenómeno contemporâneo isolado, é um elemento estruturante da modernidade, assumindo formas cada vez mais sofisticadas e invisíveis, onde a datificação da vida quotidiana emerge como o novo paradigma securitário.

Este artigo permitiu compreender como se têm edificado imaginários otimistas em torno do potencial transformador das tecnologias, imaginários esses que moldam tanto a temporalidade quotidiana presente como as projeções futuras da segurança e do policiamento. A crença na infalibilidade dos algoritmos e na neutralidade da *big data* sustenta narrativas que legitimam a sua incorporação maciça nas dinâmicas securitárias, mascarando os riscos e as implicações sociais subjacentes. A disseminação desta lógica tecno-otimista conduz à normalização da vigilância algorítmica como uma prática inevitável, relegando para um plano secundário os debates sobre direitos fundamentais, privacidade e desigualdades estruturais.

O mapeamento histórico das tecnologias de vigilância permite-nos, inspirados em Foucault (1975/1999), desenvolver uma história do presente que ilumina os processos pelos quais a vigilância se enraíza nas instituições e nas práticas sociais. O passado das tecnologias de controlo não desaparece, antes, ressurge sob novas roupagens, incorporando-se em infraestruturas cada vez mais sofisticadas e opacas — frequentemente *black-boxed* (Latour, 1987), ou seja, encerradas em sistemas cuja lógica de funcionamento permanece inacessível ao escrutínio público. A ascensão do policiamento preditivo e das ferramentas de análise de risco baseadas em *big data* não representa, portanto, uma rutura absoluta com os modelos anteriores, mas sim a sua adaptação a um contexto de hiperconetividade e de ampliação das bases de dados globais.

Neste sentido, torna-se crucial interrogar os impactos éticos e políticos dessa nova arquitetura de vigilância. A fusão entre vigilância em massa e vigilância direcionada dissolve as fronteiras entre suspeitos e não suspeitos, promovendo um modelo securitário que opera sob a lógica da coletivização da suspeição e da monitorização permanente. As implicações deste fenómeno são profundas: a transformação do policiamento num exercício algorítmico de previsão do crime desloca o foco da compreensão dos fatores sociais e estruturais que produzem a criminalidade para um modelo probabilístico que classifica corpos e territórios em termos de risco. Tal deslocamento acarreta o perigo da cristalização de desigualdades históricas, na medida em que os algoritmos, treinados sobre dados passados, tendem a reproduzir os enviesamentos e discriminações sistémicas existentes (Brayne, 2017).

A análise sumária do caso português ilustra como a adoção dessas tecnologias não ocorre num vácuo, mas antes se inscreve num processo histórico de modernização securitária, onde a tecnologia é frequentemente apresentada como a solução para desafios estruturais e políticos. A implementação de bases de dados genéticos e a expansão dos circuitos de videovigilância no país refletem não apenas um reforço do controlo social, mas também um desejo de alinhamento com padrões internacionais de segurança, muitas vezes, sem um debate aprofundado sobre as suas implicações sociais e éticas. Neste contexto, importa refletir criticamente sobre as trajetórias futuristas que se projetam relativamente ao uso de *big data* no policiamento e na investigação criminal. Que tipo de sociedade está a ser construída quando as decisões securitárias passam a ser mediadas por cálculos algorítmicos que operam de forma opaca e sem escrutínio democrático? Como garantir que as promessas de maior eficiência e previsibilidade não resultem em formas sofisticadas de exclusão e criminalização de determinados grupos sociais? Paradoxalmente, essa vigilância silenciosa e automatizada pode coexistir com formas de controlo ostensivo e altamente visível, dirigidas a populações racializadas ou marginalizadas, como ilustram intervenções policiais mediáticas em espaços urbanos associados à diferença cultural, como o caso da rua do Benformoso, em Lisboa (Neves, 2024).

Portanto, as tendências atuais sugerem que estamos a caminhar para um modelo de governança securitária marcado pela intensificação da vigilância digital, cada vez mais impercetível e integrada em infraestruturas técnicas que escapam ao controlo direto dos cidadãos e, por vezes, até dos próprios agentes de segurança.

Todavia, é necessário ter em conta que esta lógica de invisibilidade e automatização coexiste com formas públicas e altamente visíveis de controlo, muitas vezes dirigidas a populações marginalizadas, revelando um campo securitário profundamente assimétrico, onde diferentes regimes de visibilidade são seletivamente aplicados. Não obstante, importa também reconhecer o surgimento de formas de contravigilância ou *sousveillance* (Mann et al., 2003), nas quais cidadãos recorrem a tecnologias para monitorizar as ações de forças de segurança. Um exemplo paradigmático são as *bodycams*, cuja ambivalência tem sido discutida por autores como Diana Miranda (2022), ao evidenciar como estas tecnologias podem simultaneamente reforçar a transparência e aprofundar a vigilância. Paralelamente, fenómenos como o *citizen journalism* — em que cidadãos documentam e publicam interações policiais — têm vindo a alterar a visibilidade do policiamento e a relação entre vigilância e poder (Goldsmith, 2010; Huey & Broll, 2012).

Deste modo, torna-se essencial reivindicar um debate público robusto sobre os limites da vigilância digital, a transparência dos sistemas algorítmicos e a necessidade de garantir mecanismos de regulação e responsabilização. Se a vigilância algorítmica redefine os contornos do policiamento e da justiça criminal, cabe-nos interrogar as suas consequências e resistir à sua aceitação acrítica. A história da vigilância não é apenas a história do poder e do controlo, mas também a história das lutas pela liberdade, pelo direito à privacidade e pela construção de sociedades mais justas. Ao compreender o passado da vigilância, podemos questionar o seu futuro e, mais importante, desafiar as inevitabilidades tecnológicas que nos são frequentemente impostas como progresso incontestável.

Agradecimentos

A autora expressa a sua gratidão à Professora Helena Machado, orientadora científica do trabalho de doutoramento que serviu de base à análise apresentada neste artigo, assim como aos revisores, cujos comentários construtivos contribuíram significativamente para a melhoria da qualidade do texto.

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).

Este trabalho é financiado por fundos nacionais através da FCT – Fundação para a Ciência e a Tecnologia, I.P., no âmbito do projeto UIDB/00736/2020 (financiamento base) e UIDP/00736/2020 (financiamento programático).

Referências

Afzal, M., & Panagiotopoulos, P. (2024). *Data in policing: An integrative review. International Journal of Public Administration*, 1–20. https://doi.org/10.1080/01900692.2024.2360586

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, *28*(6), 24–43. https://doi.org/10.1177/0263276411417430

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

Baird, T. (2018). Interest groups and strategic constructivism: Business actors and border security policies in the European Union. *Journal of Ethnic and Migration Studies*, *44*(1), 1–19. https://doi.org/10.1080/1369183X.2017.1316185

Ball, K., & Webster, F. (2003). The intensification of surveillance. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information era* (pp. 1–15). Pluto Press.

Beck, U. (2002). The terrorist threat: World risk society revisited. *Theory, Culture & Society*, *19*(4), 39–55. https://doi.org/10.1177/0263276402019004003

Bentham, J. (1995). *The panoptic writings*. Verso Trade.

Bigo, D. (2006). Globalized (in)security: The field and the ban-opticon. In D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty. Illiberal practices of liberal regimes after 9/11* (pp. 10–48). Routledge.

Blount, K. (2024). Using artificial intelligence to prevent crime: Implications for due process and criminal justice. *AI & SOCIETY*, *39*, 359–368. https://doi.org/10.1007/s00146-022-01513-z

Bogard, W. (1996). *The simulation of surveillance: Hyper-control in telematic societies*. Press Syndicate of the University of Cambridge.

Bogard, W. (2006). Welcome to the society of control: The simulation of surveillance revisited. In K. Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 55–78). ACUP.

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/10.1177/0003122417725865

Brayne, S. (2022). The banality of surveillance. *Surveillance & Society*, *20*(4), 372–378. https://doi.org/10.24908/ss.v20i4.15946

Bunyan, T. (2010). Just over the horizon: The surveillance society and the state in the EU. *Race & Class*, *51*(3), 1–12. https://doi.org/10.1177/0306396809354162

Bygrave, L. A. (2002). *Data protection law. Approaching its rationale, logic, and its limits*. Kluwer Law International.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias. (2021). P*arecer sobre a Proposta de Lei n.º 111/XIV/2.ª (GOV) – Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança*. Assembleia da República.

Comissão Nacional de Proteção de Dados. (s.d.). *O que somos e quem somos*. Retirado a 3 de novembro de 2022, de https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

Corbett, R., & Marx, G. T. (1991). Critique: No soul in the new machine: Technofallacies in the electronic monitoring movement. *Justice Quarterly*, *8*(3), 399–414. https://doi.org/10.1080/07418829100091111

Costa, S., Machado, H. C., & Nunes, J. A. (2002). O ADN e a justiça: A biologia forense e o direito como mediadores entre a ciência e os cidadãos. In M. E. Gonçalves (Ed.), *Os portugueses e a ciência* (pp. 199–233). Dom Quixote.

Creemers, N. (2021). *The policing assemblage: On the co-evolution of technology, knowledge, and policing in New York City*. Technische Universität Berlin.

Cukier, K. N., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, *92*(3), 28–40.

Cunha, M. I. (2008). Disciplina, controlo, segurança: No rasto contemporâneo de Foucault. In C. Frois (Ed.), *A sociedade vigilante: Ensaios sobre privacidade, identificação e vigilância* (pp. 67–81). Imprensa de Ciências Sociais.

de Laat, P. B. (2019). The disciplinary power of predictive algorithms: A Foucauldian perspective. *Ethics and Information Technology*, *21*, 319–329. https://doi.org/10.1007/s10676-019-09509-y

Decisão 2008/615/JAI do Conselho, de 23 de Junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. (2008). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32008D0615

Decisão 2008/616/JAI do Conselho, de 23 de Junho de 2008 , referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras. (2008). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/eli/dec/2008/616/oj/?locale=pt

Deleuze, G. (2006). Postscript on the societies of control. In D. Wilson & C. Norris (Eds.), *Surveillance, crime and social control* (pp. 35–39). Routledge.

Deleuze, G., & Guattari, F. (1987). Introduction: Rhizome. In G. Deleuze & F. Guattari (Eds.), *A thousand plateaus* (pp. 3–28). University of Minnesota Press.

Dencik, L. (2022). The datafied welfare state: A perspective from the UK. In A. Hepp, J. Jarke, & L. Kramp (Eds.), *New perspectives in critical data studies: The ambivalences of data power* (pp. 145–166). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-96180-0_7

Durão, S. (2009). La producción de mapas policiales: Prácticas y políticas de la policía urbana en Portugal. *Intersecciones en Antropología*, *10*(1), 43–61.

Duxbury, S. W., & Andrabi, N. (2022). The boys in blue are watching you: The shifting metropolitan landscape and big data police surveillance in the United States. *Social Problems*, *71*(3), 912–937. https://doi.org/10.1093/socpro/spac044

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. University of Toronto Press.

Esposti, S. D. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance and Society*, *12*(2), 209–225. https://doi.org/10.24908/ss.v12i2.5113

Feeley, M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, *30*(4), 449–475. https://doi.org/10.1111/j.1745-9125.1992.tb01112.x

Foucault, M. (1999). *Vigiar e punir: Nascimento da prisão* (R. Ramalhete, Trad.). Vozes. (Trabalho original publicado em 1975)

Foucault, M. (2003). *Society must be defended: Lectures at the Collège de France, 1975-76*. Picador.

Foucault, M. (2008). T*he birth of biopolitics: Lectures at the Collège de France, 1978-79*. Palgrave Macmillan.

Frois, C. (2008). Vigilância e identidade: Para uma nova antropologia da pessoa. In C. Frois (Ed.), A *sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade* (pp. 175–191). Imprensa de Ciências Sociais.

Frois, C. (2013). *Peripheral vision. Politics, technology and surveillance*. Berghahn Books.

Frois, C. (2014). Video-surveillance and the political use of discretionary power in the name of security and defence. In M. Maguire, C. Frois, & N. Zurawski (Eds.), *The anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control* (pp. 45–61). Pluto Press.

Frois, C., & Machado, H. (2016). Modernization and development as a motor of polity and policing. In B. Bradford, B. Jauregui, I. Loader, & J. Steinberg (Eds.), *The SAGE handbook of global policing* (pp. 391–405). SAGE.

Gandy, O. (2006). Data mining, surveillance, and discrimination in the post-9/11 environment. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 363–384). University of Toronto Press.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. O'Reilly.

Garland, D. (1997). Governmentality and the problem of crime: Foucault, criminology, sociology. *Theoretical Criminology*, *1*(2), 173–214. https://doi.org/10.1177/1362480697001002002

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford University Press.

Goldsmith, A. (2010). Policing's new visibility. *The British Journal of Criminology*, *50*(5), 914–934. https://doi.org/10.1093/bjc/azq033

Graham, S. (2006). *Constructing 'Homeland' and 'Target' - Cities in the 'War on Terror'*. Public Culture.

Grondin, D., & Hogue, S. (2024). Person of interest as media technology of surveillance: A cautionary tale for the future of the national security state with diegetic big data surveillance, algorithmic security, and artificial intelligence. *Television & New Media*, *25*(4), 334–351. https://doi.org/10.1177/15274764231210280

Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance* (pp. 23–45). Willan.

Haggerty, K. D. (2012). Book review: The New Social Control: The Institutional Web, Normativity and the Social Bond. *Theoretical Criminology*, *16*(4), 527–531. https://doi.org/10.1177/1362480612454951

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. B*ritish Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Haggerty, K. D., & Ericson, R. V. (2007). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 3–26). University of Toronto Press.

Hu, M. (2015). Small data surveillance v. big data cybersurveillance. *Pepperdine Law Review*, *42*(4), 773–844.

Huey, L., & Broll, R. (2012). 'All it takes is one TV show to ruin it': A police perspective on police-media relations in the era of expanding 'citizen journalism'. *Policing and Society*, *22*(4), 384–396. https://doi.org/10.1080/10439463.2011.641556

Innes, M. (2003). *Understanding social control: Deviance, crime and social order*. Open University Press.

Innes, M., Fielding, N., & Cope, N. (2005). "The appliance of science?": The theory and practice of crime intelligence analysis. *British Journal of Criminology*, *45*(1), 39–57. https://doi.org/10.1093/bjc/azh053

Joh, E. (2016). The new surveillance discretion: Automated suspicion, big data, and policing. *Harvard Law & Policy Review*, 1–33.

Justice and Home Affairs Committee. (2022). *Technology rules? The advent of new technologies in the justice system*. Westminster.

Kirby, S., & Keay, S. (2021). *Improving intelligence analysis in policing*. Routledge.

Kruse, C. (2010). Forensic evidence: Materializing bodies, materializing crimes. *European Journal of Women's Studies*, *17*(4), 363–377. https://doi.org/10.1177/1350506810377699

Latour, B. (1987). *Science in action. How to follow scientists and engineers through society*. Harvard University Press.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Polity Press.

Lyon, D. (2001a). Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology*, *3*(3), 171–180. https://doi.org/10.1023/A:1012227629496

Lyon, D. (2001b). *Surveillance society: Monitoring everyday life*. Open University Press.

Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, *19*(2), 135–149. https://doi.org/10.1177/0268580904042897

Lyon, D. (2014a). Situating surveillance: History, technology, culture. In K. Boersma, R. Van Brakel, C. Fonio, & P. Wagenaar (Eds.), *Histories of State surveillance in Europe and beyond* (pp. 32–46). Routledge.

Lyon, D. (2014b). Surveillance, Snowden, and big data: Capacities, consequences, critique. B*ig Data and Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance and Society*, *13*(2), 139–152. https://doi.org/10.24908/ss.v13i2.5363

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics* (pp. 64–77). Routledge. https://doi.org/10.4324/9781315167305-4

Lyon, D. (2022). Surveillance. *Internet Policy Review*, *11*(4), 1–19. https://doi.org/10.14763/2022.4.1673

Machado, H. (2021). O futuro incerto e as turbulências da vigilância genética na Europa. In H. Machado (Ed.), *Crime e tecnologia: Desafios culturais e políticos para a Europa* (pp. 23–40). Afrontamento.

Machado, H., & Frois, C. (2014). Aspiring to modernization: Historical evolution and current trends of State surveillance in Portugal. In K. Boersma, R. Van Brakel, C. Fonio, & P. Wagenaar (Eds.). *Histories of State surveillance in Europe and beyond* (pp. 65-78). Routledge.

Machado, H., & Santos, F. (2012). Entre a polícia ficcional e a polícia real: Os usos do DNA na investigação criminal em Portugal. In S. Durão & M. Darck (Eds.). *Polícia, segurança e ordem pública: Perspetivas portuguesas e brasileiras* (pp. 201–216). Imprensa de Ciências Sociais.

Machado, H., & Santos, F. (2016). Culturas de objetividade, epistemologias cívicas e o suspeito transnacional. Uma proposta para mapeamentos teóricos em estudos sociais da genética forense. In C. Fonseca, F. Rohden, P. S. Machado, & H. S. Paim (Eds.), *Antropologia da ciência e da tecnologia: Dobras reflexivas* (pp. 179–203). Editora Sulina.

Maciel, D., & Machado, H. (2014). Biovigilância e governabilidade nas sociedades da informação. In H. Machado & H. Moniz (Eds.), *Bases de dados genéticos forenses: Tecnologias de controlo e ordem social* (pp. 141–166). Coimbra Editora.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331–355. https://doi.org/10.24908/ss.v1i3.3344

Marx, G. T. (1988). *Undercover police surveillance in America*. University of California Press.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, *1*(1), 9–29. https://doi.org/10.24908/ss.v1i1.3391

Marx, G. T. (2006). Varieties of personal information as influences on attitudes towards surveillance. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 79–110). University of Toronto Press.

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/10.1177/1362480697001002003

McCahill, M. (2022). Theorizing surveillance in the pre-crime society. In B. A. Arrigo & B. Sellers (Eds.), *The pre-crime society: Crime, culture and control in the ultramodern age* (pp. 227–267). Bristol University Press.

McQuade, B. (2021). World histories of big data policing: The imperial epistemology of the police-wars of U.S. hegemony. *Journal of World-Systems Research*, *27*(1), 109–135. https://doi.org/10.5195/jwsr.2021.1033

Miller, K. (2014). Total surveillance, big data, and predictive crime technology: Privacy's perfect storm. J*ournal of Technology Law & Policy*, *19*(1), 105–146.

Miranda, D. (2020). Identifying suspicious bodies? Historically tracing criminal identification technologies in Portugal. *Surveillance & Society*, 1–22.

Miranda, D. (2022). Body-worn cameras 'on the move': Exploring the contextual, technical and ethical challenges in policing practice. *Policing and Society*, *32*(1), 18–34. https://doi.org/10.1080/10439463.2021.1879074

Monahan, T. (2010). *Surveilllance in the time of insecurity*. Rutgers University Press.

Monar, J. (2008). The European Union as a collective actor in the fight against post-9/11 terrorism: Progress and problems of a primarily cooperative approach. In M. Gani & P. Mathew (Eds.), F*resh perspectives on the 'war on terror'* (pp. 209–234). The Australian National University Press.

Neiva, L. (2020). *Big data na investigação criminal: Desafios e expectativas na União Europeia*. 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]. RepositóriUM. https://hdl.handle.net/1822/93930

Neves, C. S. (2024, 19 de dezembro). *Dispositivo policial reforçado. Rixa na Rua do Benformoso fez vários feridos*. RTP Notícias. https://www.rtp.pt/noticias/pais/dispositivo-policial-reforcado-rixa-na-rua-do-benformoso-fez-varios-feridos_n1626944

Newburn, T. (2012). The future of policing. In T. Newburn (Ed.), *Handbook of policing* (2.ª ed., pp. 824–841). Willan Publishing.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Berg.

Norris, C., & McCahill, M. (2006). CCTV: Beyond penal modernism? *British Journal of Criminology*, *46*(1), 97–118. https://doi.org/10.1093/BJC/AZI047

Nunes, J. A., & Gonçalves, M. E. (2001). Introdução. In J. A. Nunes & M. E. Gonçalves (Eds.), E*nteados de Galileu? A semiperiferia no sistema mundial da ciência* (pp. 13–31). Afrontamento.

Pimentel, I. F. (2024). O 25 de Abril de 1974 e a PIDE/DGS. *Revista Crítica de Ciências Sociais*, (133), 121–146. https://doi.org/10.4000/11pr5

Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Polity Press.

Prainsack, B., & Toom, V. (2010). The Prüm regime: Situated dis/empowerment in transnational DNA profile exchange. *The British Journal of Criminology*, *50*(6), 1117–1135. https://doi.org/10.1093/bjc/azq055

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

Procuradoria-Geral Regional de Lisboa. (s.d.). *Legislação*. Ministério Público Portugal. Retirado a 27 de stembro de 2022, de https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1506&tabela=leis

Recomendação n.º R (92) 1. (1992). Comité de Ministros aos Estados-membros sobre a utilização da análise de ADN no âmbito do sistema de justiça penal, de 10 de fevereiro de 1992.

Ribeiro, M. C. (2004). *Uma história de regressos: Império, guerra colonial e pós-colonialismo*. Afrontamento.

Park, R. E., & Burgess, E. W. (1925). *The city*. The 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). Routledge.

Sachoulidou, A. (2023). Going beyond the "common suspects": To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-023-09347-w

Schafer, J. A., Buerger, M. E., Myers, R. W., Jensen, C. J., III, & Levin, B. H. (2011). *The future of policing: A practical guide for police managers and leaders*. CRC Press.

Schweitzer, N. J., & Saks, M. J. (2007). The CSI effect: Popular fiction about forensic science affects the public's expectations about real forensic science. *Jurimetrics Journal*, *47*, 357–364.

Skinner, D. (2018). Race, racism and identification in the era of technosecurity. *Science as Culture*, *29*(1), 1–23. https://doi.org/10.1080/09505431.2018.1523887

Strauß, S. (2018). Big data – Within the tides of securitisation? In A. R. Sætnan, I. Schneider, & N. Green (Eds.), T*he politics and policies of big data* (pp. 46–67). Routledge.

Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technology-Led Policing: Journal of Police Studies*, *3*(20), 163–192.

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*, *24*(1) 91–109. https://doi.org/10.1177/13624806241246267

Volkwein, C. E. (2022). Digitizing the fourth amendment: Privacy in the age of big data policing. *Privacy Certificate Student Publications*, *5*, 1–21.

War Studies KCL. (2022, 19 de janeiro). *How are emerging technologies (re)shaping the security landscape?* [Vídeo]. YouTube. https://www.youtube.com/watch?v=aQv9p6rCLDw

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Nota Biográfica

Laura Neiva é professora auxiliar convidada no Departamento de Sociologia do Instituto de Ciências Sociais da Universidade do Minho; e investigadora colaboradora no Centro de Estudos de Comunicação e Sociedade do Instituto de Ciências Sociais da Universidade do Minho, Portugal e no Centro de Estudos Jurídicos, Económicos e Ambientais da Universidade Lusíada Norte, Porto, Portugal. É licenciada em Criminologia, pela Faculdade de Direito da Universidade do Porto (2017), mestre em Crime, Diferença e Desigualdade, pelo Instituto de Ciências Sociais da Universidade do Minho (2019), e doutora em Sociologia também pelo Instituto de Ciências Sociais da Universidade do Minho (2024). Autora do livro *Big Data na Investigação Criminal: Desafios e Expectativas na União Europeia* (Editora Húmus), os seus interesses de investigação concentram-se nos estudos sociais da ciência e tecnologia, novas tecnologias de investigação criminal, big data, estudos da vigilância, policiamento e expectativas.

ORCID: https://orcid.org/0000-0002-1954-7597
Email: lauraneiva@ics.uminho.pt
Morada: Campus de Gualtar. Rua da Universidade, 4710-057, Braga, Portugal

Submetido: 21/02/2025 | Aceite: 31/03/2025