Capítulo 3.

BIG DATA E VIGILÂNCIA POLICIAL: DESAFIOS ÉTICOS, LEGAIS E SOCIAIS

Laura Neiva

Introdução

A existência de bases de dados e de plataformas tecnológicas com capacidade de agregar grandes conjuntos de dados não é uma realidade nova. O surgimento do termo «Big Data» – «megadados» ou «grandes dados» em português – remonta aos anos 90. Inicialmente, referia-se a volumes de informações impossíveis de serem processados pelos meios tecnológicos da época (Cukier & Mayer-Schonberger, 2013). Com o desenvolvimento da internet e das novas tecnologias informáticas, verificou-se, gradualmente, a sofisticação de meios que permitem a recolha de maiores volumes de dados, exacerbando-se as capacidades tecnológicas de produzir, partilhar e organizar os mesmos (Boyd & Crawford, 2012; Halford & Savage, 2017; Jahanian, 2014). O termo Big Data é usado frequentemente para se referir a uma área de conhecimento que desenvolve técnicas que integram grandes conjuntos de dados. Estas ferramentas analisam e processam grandes volumes de informações diversas, correlacionando-as, com o objetivo de nortear ações e decisões em diferentes esferas da vida social (Hu, 2015).

Paralelamente, também no sistema de justiça criminal se verifica, atualmente, um desenvolvimento exponencial destas novas tecnologias ao serviço da vigilância e da investigação criminal (Egbert, 2019; Lyon, 2004; Moses & Chan, 2018; Quijano-Sánchez & Camacho-Collados, 2018; Williams & Johnson, 2004). Agências governamentais, organizações de segurança e de policiamento enfrentam desafios que obrigam a uma reconfiguração dos paradigmas[1]

(1) Kuhn (2012) define um paradigma como uma forma aceite de aplicar um conhecimento produzido por um número considerável de investigadores. Neste contexto, paradigma refere-se ao modo geral de atuação de combate ao crime.

tradicionais de combate ao crime (Mantello, 2016). Consequentemente, verifica-se o desenvolvimento de novas técnicas digitais que permitam adequar-se às mudanças que a criminalidade tem sofrido (Drewer & Miladinova, 2017). Acontecimentos como o 11 de setembro de 2001 (Innes, 2001; Mantello, 2016; Williams & Johnson, 2004) e, posteriormente, os ataques terroristas em Madrid em 2004 e Paris em 2015, estimularam um maior investimento governamental em programas de segurança e vigilância sustentados em lógicas de prevenção do terrorismo. A governabilidade do crime orienta-se cada vez mais por lógicas preditivas, que visam antecipar o perigo antes que este seja uma ameaça real (Mantello, 2016).

Neste contexto, as ferramentas de Big Data têm vindo a ser encaradas como promissoras e de elevada eficácia no campo do policiamento e promoção da segurança pública (Chan & Moses, 2017). Neste contexto, estas técnicas são usadas para analisar e processar enormes quantidades de dados, produzindo correlações numéricas, com o objetivo de orientar decisões de política criminal (Brayne, 2017; Chan & Moses, 2017; Joh, 2014; Ridgeway, 2018). Atualmente, encontram aplicação prática em Departamentos Policiais nos Estados Unidos da América (Brayne, 2017), África do Sul (Joh, 2014), e Austrália (Chan & Moses, 2017).

No contexto do policiamento europeu, os dispositivos de Big Data encontram-se em fase precoce de implementação (Drewer & Miladinova, 2017; Kubler, 2017; Neiva, 2020b; Pereira, 2019). No entanto, a expansão de estratégias de governabilidade criminal assentes nestas técnicas potencia o alcance da vigilância em áreas quotidianas que antigamente eram inimagináveis (Mantello, 2016). Este aumento exponencial de estratégias vigilantes decorrentes da utilização de Big Data aprofunda uma crescente recolha massiva de informação sobre os cidadãos, caminhando-se assim para aquilo que autores como Lyon (1992) e Marx (2002) têm vindo a descrever como sociedades de segurança e controlo máximos.

No presente capítulo as técnicas de Big Data serão analisadas como uma ferramenta que expande os mecanismos de controlo e vigilância já existentes, criando uma nova modalidade daquilo a que autores como Kevin Haggerty e Richard Ericson designaram de «composição da vigilância» (*surveillant assemblage*) (Haggerty & Ericson, 2000, p. 606). O desenvolvimento destes mecanismos potencia, desta forma, uma proliferação da vigilância «em inúmeros contextos da vida quotidiana» (Haggerty, 2006, p. 3), expandindo-a e metamorfoseando-a tanto de modos subtis como ostensivos.

Um primeiro aspeto da composição e arquitetura da vigilância, no caso concreto dos dispositivos de Big Data aplicados ao policiamento e segurança pública

diz respeito à sua faceta desigualitária: não é universal o modo como a vigilância se dirige aos grupos sociais e os tenta disciplinar e controlar (Fiske, 1998; Haggerty & Ericson, 2000). Por se basear em dados recolhidos no âmbito de atividades de policiamento, o modo como perpetuam desigualdades sociais reflete as atividades discricionárias e estigmatizantes do sistema de justiça criminal. Concretamente, a sobre-representação de certas camadas sociais nas bases de dados criminais e policiais, como determinadas minorias étnicas e grupos social e economicamente vulneráveis, vai potenciar que as técnicas de Big Data orientem ações punitivas e controladoras sobre franjas populacionais historicamente criminalizadas pelo sistema de justiça (Brayne, 2017; Skinner, 2013, 2018a, 2018b). Além disso, simultaneamente, também expande as malhas vigilantes existentes, pois permite uma vigilância permanente e contínua sobre toda a população por via de dispositivos de controlo já desenvolvidos e aplicados anteriormente (Brayne, 2017).

O debate atual em torno do tema concentra-se nas capacidades tecnológicas dos dispositivos de Big Data como ferramentas úteis na redução das taxas de crime. No entanto, um enfoque excessivo nas suas potencialidades técnicas oblitera as questões sociais, éticas e legais que o fenómeno instiga. Nomeadamente, no que diz respeito ao seu risco de lesar direitos humanos e comprimir liberdades civis. O presente texto tem como objetivo ampliar este debate acerca da utilização do Big Data enquanto mecanismo de vigilância policial.

O capítulo encontra-se estruturado em seis partes. Num primeiro momento discute-se a abordagem tradicional concetual do Big Data, analisando as fragilidades que as suas definições apresentam. Na segunda secção, apresenta-se a contextualização das ferramentas de Big Data enquanto estratégias de vigilância, integrando esta análise no desenvolvimento de mecanismos vigilantes e seus fatores sociais e históricos. Na terceira parte, analisa-se o contexto atual de aplicação de técnicas de Big Data na esfera do policiamento e discutem-se os principais desafios suscitados por esta implementação. Na quarta secção problematizam-se as questões ético-sociais do Big Data, imbuídas no contexto do policiamento, reportando as suas vulnerabilidades. Na quinta parte analisa-se o contexto legal europeu e nacional contemporâneo do Big Data, com enfoque nas alterações legislativas que ocorreram e no vazio legal que permanece na Europa e em Portugal. Por fim, reflete-se sobre a necessidade de ampliar o debate ético-social e legal em torno do Big Data como mecanismo de vigilância e na sua utilização no âmbito do policiamento.

Big Data: uma breve definição

Apesar da definição do conceito de Big Data não ser consensual (Brayne, 2017; Chan & Moses, 2016; Kitchin, 2014), esta técnica caracteriza-se pelo tamanho e tipo de dados que agrega, capacidade de armazenamento, análises de processamento automatizadas e velocidade através da qual os dados são computorizados e examinados (Chan & Moses, 2016). A sua definição popular engloba três *V's* que caracterizam o fenómeno do Big Data por via das seguintes particularidades: volume dos dados que agrega (em termos de quantidade); variedade desses dados (provenientes de diferentes fontes em diferentes formatos); e a velocidade, sem precedentes, através da qual estes dados são processados (Degli Esposti, 2014; Hu, 2015). Os dados são frequentemente provenientes de contextos que se relacionam com atividades pessoais e uso de serviços básicos por parte dos indivíduos. Por exemplo, a utilização de dispositivos móveis como telefones, de cartões de crédito para realizar pagamentos, e de aparelhos eletrónicos que permitem o registo das suas localizações geográficas. Desta forma, as ações quotidianas individuais convertem-se em rastos digitais (Haggerty & Ericson, 2000; Halford & Savage, 2017; Kitchin, 2014) que são posteriormente quantificados e cedidos a terceiros como empresas, agências de governo e outros serviços. Gradualmente, criou-se uma digitalização social que gerou uma indústria de *metadados*[2] passíveis de serem partilhados, analisados e até comercializados (Lupton & Michael, 2017).

O surgimento desta realidade dos dados e da *datificação* – conversão de toda a informação em dados categorizáveis por via de nomes e/ou números (Cukier & Mayer-Schoenberger, 2013; Van Dijck, 2014) – intensificou-se depois do surgimento das novas tecnologias e das redes computacionais. No entanto, uma ênfase excessiva conferida ao desenvolvimento digital e, consequentemente, às capacidades tecnológicas das ferramentas de Big Data, neutraliza a compreensão do fenómeno enquanto realidade sociocultural. As definições clássicas das técnicas de Big Data ancoram algumas fragilidades. Desde logo, por se concentrarem apenas nas suas potencialidades de *software,* omitem considerações acerca de como os dados são e/ou podem ser armazenados, o modo como são partilhados, de que forma o processamento destas informações volumosas pode ser realizado e como é que dados tão diversos podem ser correlacionados (Chan & Moses, 2016).

(2) Geralmente associados a conjuntos de conhecimentos criados a partir de dados brutos, ou seja, informações sobre determinado fenómeno. A criação de *metadados* visa organizar, de forma estruturada, dados organizacionais para facilitar a sua manutenção e posterior utilização (Ikematu, 2001).

Tendo em conta que as ferramentas tecnológicas são socialmente constituídas (Lyon, 1992), os mecanismos de Big Data não podem ser compreendidos fora do seu contexto social, sendo necessário, tal como «qualquer [outro] discurso sobre uma nova vigilância, uma análise sofisticada da interação complexa entre fatores sociais e tecnológicos», de modo a identificar as consequências (não) intencionais da sua utilização (Lyon, 1992, p. 165). Sob a lente sociológica, Big Data é definido como um fenómeno cultural, social e político (Chan & Moses, 2016) que, segundo Boyd e Crawford (2012, p. 663) agrega três dimensões. Em primeiro lugar, a tecnologia: trata-se de um fenómeno eminentemente tecnológico que, tendo por base ferramentas computacionais e algorítmicas, recolhe, analisa e processa conjuntos de dados. Em segundo lugar, a sua componente analítica: as técnicas de Big Data operam por via de processos analíticos que possibilitam a identificação de relações entre variáveis que visam informar a tomada de decisões. Por último e em terceiro lugar, o seu caráter mitológico: as crenças generalizadas que circulam em torno da técnica como ferramenta infalível, objetiva e com capacidades de precisão incomparáveis (Boyd & Crawford, 2012). Nas palavras de Lyon (2014, p. 6) estes tipos de crenças apresentam-se como uma «fé quase ingénua na tecnologia que inibe a procura de alternativas». Esta mitologia, subjacente às ferramentas de Big Data, realça os imaginários sociais que surgem em torno da técnica como incontestável e capaz de produzir conhecimentos que não eram possíveis até então. No entanto, estas visões obscuram uma compreensão profunda deste fenómeno enquanto realidade sociocultural. De facto, adotar uma lente que apenas se foque no valor dos dados como números (Matzner, 2016), negligencia a compreensão do fenómeno de Big Data enquanto mecanismo de vigilância.

A nova «composição da vigilância»

Assistimos hoje à globalização[3] da vigilância, potenciada pela crescente mobilidade no tempo e espaço, convertendo-se numa realidade omnipresente nas sociedades modernas (Giddens, 1990; Lyon, 1992, 2004, 2014; Marx, 2002). As práticas de Big Data inserem-se no que Clarke (1988, p. 498) descreveu como *dataveillance*, a «vigilância dos dados», isto é, a «monitorização sistemática de pessoas ou grupos, por meio de sistemas de dados pessoais para regular ou governar os seus comportamentos» (Degli Esposti, 2014, p. 209). É o «desejo de

(3) Entende-se globalização como a expansão de ações à distância, de modo a que as relações sociais se estendem no espaço e no tempo; e o aumento da velocidade, intensidade, alcance e impacto das comunicações (Giddens, 1990; Lyon, 2004).

reunir sistemas, combinar práticas e tecnologias e integrá-las num todo maior» (Haggerty & Ericson, 2000, p. 610), denotando a crescente convergência de técnicas de vigilância autónomas e individuais que confluem para criar sistemas vigilantes globais. Portanto, enquadrar o fenómeno do Big Data enquanto nova «composição da vigilância» (Haggerty & Eriscon, 2000, p. 606), significa compreendê-lo como «um fenómeno convergente de sistemas de vigilância diversos, que abstraem corpos humanos dos seus contextos territoriais e os separa por via de fluxos individuais». Adotando a perspetiva proposta por Haggerty e Ericson (2000), as técnicas de Big Data são compreendidas como um meio de operacionalizar um aparato vigilante que monitoriza e analisa indivíduos e comportamentos humanos, transformando os seus dados individuais em códigos numéricos, por via da recolha de interações quotidianas, como trocas sociais e comerciais. Ou seja, os dispositivos de Big Data visam «marcar o corpo humano para que os seus movimentos através do espaço possam ser registados, para a reconstrução mais refinada dos hábitos, preferências e estilo de vida de uma pessoa a partir de rastos de informações» (Haggerty & Ericson, 2000, p. 611). Convertendo-se numa vigilância que reúne um volume de informações aparentemente ilimitadas, as suas análises e processamentos visam elaborar imagens categóricas ou perfis individuais de risco, tornando estes fluxos de informações compreensíveis e interpretáveis. Além disso, concetualizar os mecanismos de Big Data enquanto «composição da vigilância» (Haggerty & Ericson, 2000, p. 606) enfatiza a sua natureza dinâmica e fluída. Não existe uma agência centralizada única que coordene a totalidade dos sistemas e operações desta vigilância dos dados. Os dispositivos de Big Data têm capacidade de integrar diversos sistemas e atores de vigilância. Não obstante, este fenómeno materializa duas facetas distintas, mas uníssonas na forma como opera na vigilância. As técnicas de Big Data incorporam o caráter rizomático (Haggerty & Ericson, 2000) da vigilância porque operam por via de distintos atores e entidades descentralizados. No entanto, também são hierárquicas, porque assentam, com maior ênfase, em determinadas franjas populacionais, criando assimetrias e desigualdades no seu espetro de atuação (Brayne, 2017; Hier, 2003).

Historicamente, Michael Foucault (1977) utilizou a estrutura panótica prisional equacionada por Bentham (1995) para metaforicamente teorizar sobre as atividades da vigilância. Por via de uma estrutura física no interior das prisões, exercia-se um controlo contínuo e permanente da população reclusa. Atualmente, estas estruturas são maioritariamente invisíveis, tal como as ferramentas do Big Data, ao contrário do que sucedera com o projeto *benthaniano*. No entanto, materializam o seu racional subjacente: uma vigilância contínua e permanente sobre a globalidade. O desenvolvimento da vigilância e das bases de

dados computorizadas marcaram uma rutura decisiva na natureza e expansão das práticas primitivas de vigilância, provocando uma «descontinuidade histórica» (Manokha, 2018, p. 227) que nos obriga a repensar a metáfora panótica (Haggerty & Ericson, 2000). As estratégias da vigilância foram «auxiliadas por variações e intensidades subtis nas capacidades tecnológicas e conexões com outros dispositivos de monitorização e computação» (*idem*, p. 615), sofisticando-se e operando por meios tecnológicos. Portanto, embora o poder da vigilância contemporânea operada pelas estratégias do Big Data se insira neste racional de supervisão e controlo contínuos e permanentes, supera as limitações técnicas do panótico, por operar por via de dispositivos móveis e tecnológicos invisíveis onde «não são necessárias paredes, torres de vigia, guardas ou barreiras» (Lyon, 1992, p. 169). A ferramenta do Big Data materializa-se por via de múltiplos atores que o operacionalizam e, também, que são alvo deste controlo e monitorização vigilantes. A ideia de que «um controla todos» ofusca-se perante um método de vigilância que é exercido por várias entidades (Hier, 2003).

Adicionalmente, nesta reflexão metafórica há, pelo menos, mais dois aspetos sob os quais o Big Data se distancia do panótico vigilante (Foucault, 1977). Em primeiro lugar, o Big Data é um tipo de vigilância global e não alocado num contexto tão específico como o prisional, onde o panótico fora projetado. Em segundo lugar, o objetivo da monitorização por via da recolha, análise e processamento de conjuntos de dados individuais não é o mesmo que o modelo panótico. Esta última estratégia visava vigiar os comportamentos humanos com o objetivo de lhes incutir regras, disciplina e punições face a atitudes desviantes. No entanto, a aplicação das técnicas de Big Data não têm somente este objetivo de punição e ensinamento de boas práticas como visara o modelo panótico. O fenómeno do Big Data almeja, para além disso, controlar e vigiar os comportamentos individuais com o objetivo de inferir acerca de comportamentos futuros. Estas tecnologias dos dados repartem as ações humanas em fluxos de informações, criando perfis categóricos (Hier, 2003, p. 402), ou seja, contornos comportamentais passados que permitam aferir sobre as suas ações futuras. Por via destes mecanismos, infere-se acerca de comportamentos humanos que são invisíveis à perceção humana. A abstração dos corpos vigiados e a sua segmentação em fluxos distintos e individuais (Haggerty & Ericson, 2000) permite explorar com mais facilidade certos grupos, indivíduos ou mesmo populações que sejam consideradas como potencialmente perigosas, criminosas, terroristas ou migrantes ilegais. Desta forma, o panótico aplicado ao fenómeno do Big Data permite situar e compreender o seu desenvolvimento, mas não se trata de uma transposição uníssona do modelo para a vigilância contemporânea (Lyon, 1992), nem tão pouco para a nova «composição da vigilância» (Haggerty & Ericson, 2000, p. 606).

A vigilância dos dados (Clarke, 1988) por via de técnicas de Big Data também se diferencia de outros mecanismos vigilantes em alguns aspetos. Desde logo, amplia a vigilância tradicional (por exemplo, patrulhamento policial pedestre), exacerbando-a e operando de forma invisível. Materializando-se por via de objetos tecnológicos que contêm sensores invisíveis que registam os dados sobre os seus utilizadores (por exemplo, histórico de chamadas telefónicas e localização geográfica), oferece novas oportunidades para controlar indivíduos e comunidades em larga escala. É uma vigilância estritamente especulativa que controla e monitoriza, agregando e classificando, os dados sobre os cidadãos. Potencia a eficiência, difusão e invisibilidade de processos de vigilância já existentes, intensificando-os. Desta forma, este «novo regime unificado e dinâmico de vigilância de dados» (Raley, 2013, p. 124) caracteriza-se não só pela agregação de dados em larga escala, mas também, por este rastreamento sofisticado dos dados. Além disso, permite a partilha destes dados entre diferentes entidades com fins distintos, todas operadas por via da mesma base de dados.

Simultaneamente, a vigilância tradicional é indutiva, pois exerce controlo sobre indivíduos sob suspeita. Porém, esta nova vigilância é essencialmente dedutiva e categórica. Isto significa que os dispositivos de Big Data se materializam por via de mecanismos invisíveis, automatizados e incorporados nas rotinas dos cidadãos, sem fins pré-definidos nem suspeitas conhecidas. Ou seja, ao invés de se repousar sobre determinada suspeita, repousa sobre a globalidade da população, mesmo que as suspeitas sejam inexistentes, exerce uma monitorização permanente, constante e contínua (Hu, 2015).

Não obstante, a recolha dos dados por via das ferramentas de Big Data é automática e feita por via de dispositivos eletrónicos. No entanto, a sua implementação não decreta a extinção dos mecanismos vigilantes pré-existentes como, por exemplo, a revista pessoal, em que um agente policial fiscaliza determinado suspeito. Ou seja, além de expandir a vigilância como já referido, permite aferir deste tipo de informações de forma automática. O processo de recolha, análise e processamento de informações pessoais é uma tarefa «mais fácil» (Marx, 2002, p. 15) que a vigilância tradicional que necessita de um agente que, por exemplo, questione os indivíduos acerca do lugar onde estavam (Lyon, 1992; Marx, 2002). Com as técnicas do Big Data, esse tipo de informação é recolhido de forma automática e em poucos segundos. Esta ferramenta captura informações pessoais que permitem identificar indivíduos que, por via de outras técnicas de observação direta no local, seriam invisíveis. Desta forma, caracteriza-se por ser um instrumento «reconstrutivo» (Williams & Johnson, 2004, p. 4) que, após esta captura de informações, «os indivíduos e as suas ações não são observadas, mas são inferencialmente reconstruídas por profissionais especializados no e durante as

investigações criminais» (*idem*, p. 4). Os dados recolhidos sobre os indivíduos são categorizados numericamente, inseridos em bases de dados e processados, para serem analisados.

O desenvolvimento de novos mecanismos de vigilância possibilita, de forma crescente, que a vida quotidiana individual se torne transparente para as organizações que operam nesta vigilância. E, por sua vez, estas últimas são, crescentemente, ocultadas perante os indivíduos alvo da vigilância. Este «paradoxo» (Lyon, 2014, p. 4) exacerba-se com o surgimento do mecanismo Big Data, na medida em que se trata de uma monitorização eletrónica que agrega cada vez mais capacidades de vigilância e que torna impercetível saber quem é responsável por estas (Haggerty & Ericson, 2000).

Big Data: um mecanismo de vigilância policial

Apesar de historicamente existir a ambição, por parte das agências policiais, de combinar diferentes tipos de dados (Haggerty & Ericson, 2000), os estudos em torno da integração de análises de dados no policiamento complexificaram-se desde os primeiros debates sobre as técnicas de Big Data (Linder, 2019).

De acordo com Joh (2014, p. 42-55), os dispositivos de Big Data podem ter três potenciais aplicações nas atividades de policiamento: i) policiamento preditivo; ii) vigilância em massa; e iii) bases de dados de DNA[4]. O policiamento preditivo caracteriza-se pela identificação de indivíduos, locais e eventos com alto risco de criminalidade, tendo por base dados recolhidos no âmbito da atividade policial (Quijano-Sánchez & Camacho-Collados, 2018). Exemplos desta aplicação são o uso de tecnologias de análise de dados para efetuar previsões espaciotemporais de crimes futuros (Egbert, 2019). A vigilância em massa prevê a monitorização de vídeo-imagens de biliões de câmaras instaladas em circuitos de videovigilância amplamente difundidos em todas as cidades do mundo (Babuta, 2017). As bases de dados de DNA, que possuem informações de perfis genéticos, com o objetivo de detetar e apreender suspeitos de crimes poderão expandir-se, com a aplicação de técnicas de Big Data (Joh, 2014).

A um nível prático, a utilização de estratégias de Big Data em Departamentos Policiais ancora mudanças significativas nas atividades de aplicação da lei. No Departamento de Polícia de Los Angeles verifica-se a realização de avaliações

(4) Sigla de ácido desoxirribonucleico que, embora a sua tradução para língua portuguesa seja ADN, este capítulo utiliza a designação aprovada pela Sociedade Internacional de Bioquímica.

discricionárias individuais: tendo em conta o Certificado de Registo Criminal[5], os crimes cometidos pelos indivíduos são alvo de uma quantificação de risco, proporcional à sua gravidade (determinada pela pena atribuída pela legislação em vigor no país) permitindo a criação de índices de risco individuais. Estes índices são inseridos nas bases de dados policiais e partilháveis entre outras, para consulta, análise e intervenção. Verifica-se, também, uma crescente utilização dos dados para fins preditivos, ao invés de fins reativos. Por via da capacidade preditiva das ferramentas de Big Data, identificam-se indivíduos, locais e eventos com alto risco de crime, focando-se os esforços policiais em áreas de maior risco de ocorrência de crimes. Estas mudanças culminam numa expansão de sistemas que potenciam a monitorização sistemática de elevados números de pessoas, expandindo-se a vigilância. Em simultâneo, este dispositivo potenciou a junção de sistemas de informação que anteriormente eram tratados em separado. Por outras palavras, verifica-se uma interoperabilidade entre diferentes bases de dados, que são agora partilhadas entre diferentes Centros de Investigação Criminal e Departamentos Policiais, com o objetivo de potenciar a celeridade das atividades de aplicação da lei. Assim, a informação, proveniente de diferentes fontes (incluindo instituições não criminais), é armazenada, processada e analisada em conjunto (Brayne, 2017).

Os Departamentos Policiais em França, após os ataques terroristas de 2015 em Paris, integraram nos seus protocolos o uso de *softwares* de policiamento que materializam estratégias de Big Data. Nomeadamente, o *IBM's computer program – i2 Analyst's Notebook* que é um programa de policiamento que permite organizar e visualizar dados criminais, conectando suspeitos a crimes. Através de pesquisas que procuram encontrar associações entre estes dois últimos, atribuem-lhe uma classificação sobre a sua importância para a investigação (Kubler, 2017). A Europol[6] integrou, também, em 2017 aquando da reestruturação do seu Regulamento, as ferramentas de Big Data como medidas preventivas e preditivas para combater crimes como o cibercrime e o terrorismo (Drewer & Miladinova, 2017). Em Portugal, verifica-se a inclusão das técnicas de Big Data nos Regulamentos da Polícia de Segurança Pública (Pereira, 2019). No entanto, dada a escassez de produção científica sobre o tema, não se pode aferir da sua implementação real e concreta. Constata-se, apenas, a previsão formal de aplicação de estratégias de Big Data por via de um sistema policial em curso – Sistema Estratégico de Informação – que se caracteriza, em termos estruturais e funcio-

(5) Documento que atesta a existência de antecedentes criminais.

(6) Serviço europeu de Polícia responsável por cooperar com todos os Estados-Membros na luta contra determinados crimes, como terrorismo e cibercrime e outras formas de crime organizado (Disponível em: https://www.europol.europa.eu).

nais, pelas mesmas componentes do fenómeno Big Data. Nomeadamente, pela existência de bases de dados capazes de armazenar grandes volumes de dados diversos, a possibilidade da sua partilha com outras agências policiais e cálculo de correlações entre dados armazenados (Pereira, 2019).

No entanto, vários estudos referem que o impacto da aplicação das técnicas de Big Data nas práticas policiais pode produzir efeitos desiguais ou imprevisíveis. Alguns estudos nos Estados Unidos da América acerca da tecnologia policial demonstram que as mudanças tecnológicas são complexas e, frequentemente, produzem efeitos contrários aos esperados (ver Koper *et al.*, 2014). No Canadá, estudos realizados em seis Departamentos Policiais referem que o uso de tecnologias para apoiar o policiamento era mais teórico que prático, porque não produziu os resultados esperados (ver Sanders *et al.*, 2015). Um estudo realizado na Austrália indica que apesar dos agentes policiais reconhecerem o potencial de Big Data, afirmam que não possuem recursos económico-profissionais para beneficiar desse potencial. Os profissionais consideram que é uma técnica associada a um volume de dados que exige uma formação especializada para o seu manuseamento, revelando tendências comportamentais de resistência à adoção de uma nova técnica de investigação criminal (Chan & Moses, 2017). Um estudo realizado no Reino Unido também indica que as técnicas de Big Data não encontram aplicação prática dado que, atualmente, as bases de dados policiais estão fragmentadas. Os dados são recolhidos a partir de sistemas separados que não são mutuamente compatíveis e, portanto, a junção das diferentes bases de dados não é exequível. Além disso, a análise destes dados policiais continua a ser feita de forma manual, embora possuam um *software* disponível, não se realizam análises automatizadas. As forças policiais também não dispõem de ferramentas analíticas avançadas que lhes permitam avançar com análises de dados diferentes não estruturados (por exemplo, combinação de imagens de vídeo com dados de chamadas telefónicas). Os escassos recursos económicos dificultam, também, o desenvolvimento tecnológico policial. Por fim, as restrições ético-legais que regulamentam o uso dos dados policiais não preveem o manuseamento de estratégias de Big Data por parte dos agentes policias (Babuta, 2017). Portanto, este aparato tecnológico suscita um universo de questões éticas, sociais e legais que têm impacto na sua utilização prática nas atividades de policiamento.

Questões éticas e sociais

O modo como os dispositivos de Big Data se materializam em estratégias de vigilância policial levanta questões éticas e sociais, desde o modo de recolha dos

dados, à sua posterior utilização para nortear ações de governabilidade do crime. É, portanto, necessário «interrogar criticamente as suposições e premissas [do Big Data]» (Boyd & Crawford, 2012, p. 663).

Em primeiro lugar, no que diz respeito ao facto de Big Data recolher um grande volume de dados. Esta assunção cria um mito de que se recolhem fenómenos na sua totalidade. No entanto, esta recolha de dados não significa a apreensão de todos os dados, mas antes uma amostra destes, uma parte representativa do todo (Boyd & Crawford, 2012). Portanto, «isto [as análises do Big Data] está longe de ser uma leitura completa destes dados» (Bauman *et al.*, 2014, p. 125). Esta «fé especulativa» (Bauman *et al.*, 2014, p. 125) em torno da ideia de que uma maior quantidade de dados permite obter formas de conhecimento e de inteligência mais sofisticadas e adequadas para combater a criminalidade, ofusca o debate em torno das consequências ético-sociais e para os direitos humanos que esta técnica instiga (Boyd & Crawford, 2012).

Em segundo lugar, o processo de inserção de dados nas bases de dados do sistema de justiça não é aleatório. É resultado de um conjunto de práticas policiais históricas, sociais e culturais que podem apresentar-se como discriminatórias, determinando a forma como a vigilância depois é executada. A atuação policial pode ser guiada por estas assimetrias que se tornarão mais significativas à medida que as técnicas orientadas por dados guiarem as investigações criminais (Brayne, 2017). Os dados são recolhidos por tecnologias que os moldam e, portanto, estão sujeitos a erros de amostragem: processos que não garantem que a recolha de determinados dados corresponda aos dados na realidade. A compreensão destes dados e a sua posterior interpretação influenciam a forma como são extrapolados e posteriormente usados. Embora o processo de análise e recolha seja automático, os algoritmos[7] que processam os dados possuem valores contextualizados dentro de um paradigma definido. A interpretação é crucial para a análise dos dados e o tamanho destes está sujeito a limitações e preconceitos que, caso não sejam tidos em consideração, podem potenciar interpretações enviesadas (Boyd & Crawford, 2012).

Em terceiro lugar, as ferramentas de Big Data podem potenciar a perceção de relações inexistentes entre fenómenos. Devido ao volume de dados que agrega, produz relações entre variáveis que não têm associação (Zwitter, 2014). As correlações obtidas entre variáveis em estudo podem não possuir nenhuma associação causal e interpretá-las dessa forma pode conduzir a falácias: «Uma coisa é identificar padrões; outra é explicá-los» (Kitchin, 2014, p. 8). A explica-

(7) Construção matemática com uma estrutura finita, abstrata e eficaz, que cumpre uma determinada finalidade, sob certas disposições (Mittelstadt *et al.*, 2016).

ção de relações entre variáveis requer conhecimento acerca destas, portanto há uma necessidade de aprofundar o conhecimento em torno das conclusões obtidas por via dos dispositivos de Big Data. Na esfera do policiamento, por exemplo, partir do pressuposto de que uma determinada tipologia criminal reunirá sempre as mesmas características ao nível dos seus perpetradores, pode direcionar as investigações criminais sempre para os mesmos suspeitos (Brayne, 2017). Os fenómenos criminais são revestidos de uma complexidade e singularidade que é ofuscada pela consideração de que diferentes aspetos de natureza completamente distinta podem ser relacionados sobre a mesma aura geral (Uprichard, 2013).

Em quarto lugar, os dados não são elementos naturais e neutros, resultando de processos complexos que moldam a sua constituição. Desta forma, não são desprovidos de fatores sociais como a classe social, o género ou a raça (Boyd & Crawford, 2012) e, portanto, estas análises de dados podem (re)produzir e até a exacerbar desigualdades sociais (Brayne, 2017; Christin, 2016). No campo do policiamento, as estratégias de Big Data baseiam-se em dados policiais já recolhidos para direcionar decisões e ações de justiça criminal. A literatura refere que as atividades de policiamento são desigualmente distribuídas mediante a raça, a classe social e a área de residência, reforçando e legitimando lógicas sociais de discriminação, racialização e criminalização. Determinados grupos sociais (como minorias étnicas) e determinados locais (como bairros de classe social baixa), são mais prováveis de serem alvo deste controlo vigilante (Skinner, 2013, 2018a, 2018b). Por exemplo, a atuação policial tende a concentrar-se, com maior ênfase, em comunidades de raça negra (Beckett *et al.*, 2005). Também os indivíduos que residam em locais sinalizados como áreas residenciais de classe social baixa ou de minorias étnicas têm maior probabilidade de serem quantificados com alto nível de risco criminal, quando comparados com indivíduos residentes em locais onde a vigilância policial não é direcionada (Brayne, 2017).

Portanto, o mecanismo de Big Data materializa-se numa vigilância descendente (Hier, 2003, p. 400) que potencia estas desigualdades sociais já existentes. Este tipo de análises «estão repletas de suposições do determinismo social» (Kitchin, 2014, p. 8), ou seja, assunções que afirmam que o facto de determinado indivíduo pertencer a determinado local residencial ou possuir um histórico de infrações penais determina-o a agir consoante o sucedido nessas áreas ou no seu passado. Este tipo de decisões, que se baseiam nestas correlações, podem desencadear ciclos de atuação policial que, em última instância, prejudicarão o objetivo das intervenções (Chan & Moses, 2016). Simultaneamente, podem contribuir para a «classificação social», ou seja, produzir resultados desiguais,

tendo em conta estes fatores como a classe social, histórico criminal e/ou área de residência, a partir de técnicas supostamente neutras. Isto dá origem a «suspeitas categóricas» (Lyon, 2014, p. 10), isto é, a atividades de suspeição que repousam sobre determinadas camadas sociais. Consequentemente, as ferramentas de Big Data podem potenciar a criação de «comunidades suspeitas» (Machado *et al.*, 2020, p. 14): modos coletivos de atuação que afetam, de forma muito clara, grupos sociais vítimas de um poder discricionário por parte do sistema de justiça criminal (Machado *et al.*, 2020).

Estas assunções materializam o que Halford e Savage (2017, p. 1140) descrevem como o «viés»: resultados obtidos por via das estratégias de Big Data sobre grupos sobre-representados na pesquisa. Ou seja, determinados indivíduos, grupos e locais são alvo de um maior arsenal de vigilância, quando comparados com outros. Os estudos enfatizam de que estas análises repousam sobre suspeitos (já) registados e conotados nas bases de dados criminais. Ou seja, sobre grupos e áreas que têm histórico de fiscalização, controlo e supervisão, reforçando a sua estigmatização (Brayne, 2017). Este estigma, historicamente reforçado por estereótipos e representações sociais, pode fazer com que as correlações iniciais se tornem numa «profecia auto-realizável» (Chan & Moses, 2016, p. 33) que não apenas perpetua estereótipos e atitudes hostis por parte da polícia, mas que de facto pode aumentar a taxa de criminalidade. Estes indivíduos podem adotar uma identidade criminal, fruto dos contactos sucessivos com as instâncias da lei, reproduzindo comportamentos desviantes como resposta à assunção dessa identidade (Becker, 1963; Lemert, 1967).

Não obstante, como se verificou através dos resultados do estudo de Brayne (2017), o trabalho policial quando recaiu sobre bairros de classe social baixa conotou não só os indivíduos sinalizados, mas também as pessoas que os acompanhavam. Ou seja, esta recolha gradual de dados pessoais não só dos indivíduos sob suspeita, mas também de outras pessoas em contacto com os primeiros, facilita a inserção de novos indivíduos no sistema, potenciando o seu futuro contacto com as instâncias policiais (Brayne, 2017). Este facto denota o caráter rizomático (Haggerty & Ericson, 2000) das ferramentas de Big Data, ou seja, a sua capacidade de alargar a malha vigilante sobre a população. Haggerty e Ericson (2000, p. 606) referem que no processo de expansão da vigilância, os grupos que não eram alvos desta vigilância, estão continua e progressivamente a ser integrados nestes novos sistemas vigilantes.

Estes processos são potenciados pela existência de bases de dados capazes de armazenar grandes quantidades de informações e que podem ser pesquisadas retrospetivamente (Andrejevic & Gates, 2014). Na prática, reproduzem-se duas consequências: i) dados digitais recolhidos de indivíduos inocentes podem

vir a ser vinculados a cenas de crime; e ii) perpetuam contactos sucessivos dos indivíduos com o sistema de justiça criminal, visto que ficam sempre vinculados a um determinado local, crime ou comportamento desviante (Williams & Johnson, 2004). Estes processos potenciam uma «vigilância prospetiva» (Matzner, 2016, p. 199) em dois prismas: as bases de dados são armazenadas e podem ser usadas para fins de vigilância a qualquer momento no futuro; e vincula, permanentemente, os perpetradores de atos criminais ao seu próprio historial de crime, na medida em que os seus dados ficam armazenados nas bases de dados. Desta forma, o fenómeno do Big Data (re)produz dois impactos no âmbito da vigilância. Por um lado, pode perpetuar desigualdades sociais por acentuar a vigilância sobre determinadas «comunidades suspeitas» (Machado *et al.*, 2020, p. 14). Por outro lado, amplia as malhas da vigilância já existentes, recaindo sobre a população como um todo, edificando um «mundo de potenciais suspeitos[8]» (Hu, 2015, p. 606).

Por fim, determinadas dinâmicas sociais informam o modo como os dados que orientam decisões e ações de justiça criminal são, frequentemente, distorcidos, orientando estratégias de atuação policial assimétricas. Nomeadamente, crimes que não são reportados e, portanto, estão fora do alcance policial[9], não integrando a equação algorítmica que orientará uma ação policial, pelo que a sua resolução permanecerá inexistente. Também os crimes que ocorrem em locais privados que são menos visíveis para a polícia e, portanto, não são registados (Joh, 2017). Desta forma, os sistemas de policiamento baseados nos dados são «tão bons quanto os dados que eles possuem» (Joh, 2017, p. 300). Estas realidades podem contribuir para assimetrias na atuação policial que podem colocar em causa direitos e liberdades fundamentais.

Desafios legais

Os mecanismos de Big Data estão imbuídos num processo de «retórica utópica e distópica» (Boyd & Crawford, 2012, p. 663) na medida em que podem ser

(8) Considera-se «suspeito» como subgrupos populacionais que são alvo de atenção estatal por serem considerados problemáticos. No que toca às atividades policiais, os indivíduos são alvo de vigilância e controlo devido à suspeita de participação em grupos suspeitos (Pantazis & Pemberton, 2009).

(9) Os dados criminais inseridos nas bases de dados policiais dizem respeito à criminalidade que é reportada ao Sistema de Justiça Criminal. O registo de um crime depende de um processo de várias etapas desde a denúncia, à queixa, ao prosseguimento com a queixa, à sua classificação e posteriores fases de julgamento, portanto muitas vezes a criminalidade reportada não coincide com a efetiva (ver Joh, 2017).

considerados sob dois prismas: por um lado, ferramentas valiosas capazes de lidar com várias problemáticas em áreas tão diferentes como a medicina, a investigação criminal e o comércio; por outro lado, a manifestação do *Big Brother*, permitindo violações à privacidade, restringindo liberdades civis e potenciando o controlo do Estado (Boyd & Crawford, 2012; Coll, 2014; Herschel & Miori, 2017). Desde os primeiros ensaios sobre a temática que os focos argumentativos se debruçam sobre as implicações que a vertente tecnológica de Big Data tem nos direitos, garantias e liberdades fundamentais. Tal como Lyon (1992, p. 160) afirma: «as novas tecnologias facilitam a violação dos direitos das pessoas», instigando questões jurídicas profundas (Bauman *et al.*, 2014).

São vários os estudos das ciências sociais que enfatizam os impactos negativos que a técnica de Big Data pode acarretar na esfera dos direitos humanos (ver Ball *et al.*, 2016; Boyd & Crawford, 2012; Brayne, 2017; Coll, 2014; Gonçalves, 2017; Herschel & Miori, 2017; Lyon, 2014; Mantelero, 2017; Metcalf & Crawford, 2016; Mittelstadt *et al.*, 2016; Richardson *et al.*, 2019). Fruto de um desenvolvimento tecnológico que supera, em larga escala, as respostas legais e regulamentares que existem neste novo paradigma digital, a ferramenta do Big Data reconfigurou a vigilância e o quotidiano social. Desta forma, os esforços em torno das intervenções legislativas devem acompanhar este processo (Andrejevic & Gates, 2014). Ou seja, redefinir os padrões de privacidade e proteção de dados, o que obrigará a adaptações legais e regulamentares por parte das várias agências, Estados e instâncias governamentais (Mantelero, 2017). Isto não significa que, atualmente, qualquer processamento de dados pessoais é sempre considerado uma violação ao direito à privacidade, mas antes que esse processamento de dados pessoais se efetive por via de certas condições legais, sob pena de se lesarem direitos, liberdades e garantias (Neiva, 2020b).

Na esfera dos direitos humanos, o direito à privacidade e proteção de dados são os lesados na era digital contemporânea. Submersos num universo de vigilância dos dados omnipresente (Clarke, 1988), é um desafio a forma como podem ser salvaguardados (Mann & Matzner, 2019; McDermott, 2017). No que diz respeito ao direito à privacidade, trata-se de um direito humano internacional abrangente que está previsto na Declaração Universal dos Direitos Humanos da Organização das Nações Unidas (1948) e no Pacto Internacional das Nações Unidas sobre Direitos Civis e Políticos (1966). Estes documentos legais referem, a este propósito, que qualquer intromissão na privacidade de uma pessoa deve estar sujeita ao consentimento desta. Ou seja, o uso dos dados pessoais é decidido pelo titular dos dados. Este aspeto limita os propósitos da recolha e uso de dados pessoais dos cidadãos. Caso existam situações de recolha

e uso destes dados, estas devem ser permitidas por lei, de forma clara e pública, para que os indivíduos tenham conhecimento delas e possam ajustar o seu comportamento ao que sucederá. Além disso, a recolha deve cumprir um objetivo legítimo e necessário.

Contudo, na prática, estes princípios enfrentam alguns desafios. Desde logo, porque a técnica de Big Data não recolhe dados sobre uma única pessoa, mas também sobre as pessoas que contactam com estas, logo a justificação desta intromissão individual é uma tarefa desafiadora (Bauman *et al.*, 2014). Além disso, a omnipresença de dados voluntários cedidos por via do uso de dispositivos móveis e redes sociais alimenta o raio de recolha destes dados, sendo árduo definir o tipo de dados a recolher para cumprir os fins destinados. E, por fim, embora o objetivo legítimo e necessário da recolha de dados seja a garantia da segurança nacional, o equilíbrio entre este e a preservação dos direitos humanos continua(rá) a ser objeto de debate. Relativamente a este aspeto, as técnicas de vigilância em massa são consideradas pelo Tribunal Europeu dos Direitos Humanos como inconsistentes com o direito à privacidade, estabelecendo-se uma justificação rigorosa por parte das entidades que acedem aos dados, explicando a razão de o fazer, salvaguardando-se o respeito pelos direitos da Convenção dos Cidadãos (Vermeulen & Lievens, 2017). Este aspeto reforça a necessidade de rever o estado legal da proteção de dados e da privacidade (Bauman *et al.*, 2014).

No entanto, embora o fenómeno do Big Data instigue mudanças tectónicas no universo legislativo, salienta-se um esforço legal na criação de documentos que reforcem o Estado de direito. O Conselho Europeu procedeu a uma revisão de programas que procurou responder às ansiedades práticas de um sistema democrático. Concretamente, referiu que a forma célere como esta rápida evolução da tecnologia reconfigura o mundo à nossa volta exige emergentes respostas a questões como proteção de dados pessoais, privacidade e consentimento (Gonçalves, 2017). Consequentemente, no que diz respeito à proteção de dados, procedeu-se à reforma da Diretiva de Proteção de Dados de 1995 com a implementação do Regulamento da União Europeia 2016/679 (Conselho da União Europeia, 2016a), integrando-se nesta o desenvolvimento tecnológico e as novas tecnologias como uma categoria de aplicações digitais a serem incluídas no arsenal do regime de proteção de dados (McDermott, 2017). Também a Europol procedeu a alterações no seu Regulamento, no que concerne à criação de um quadro jurídico que equilibre os interesses fundamentais de liberdade, proteção de dados e segurança, após a previsão de Big Data como estratégia de combate ao crime (Drewer & Miladinova, 2017).

Foi, também, publicada uma Diretiva na União Europeia[10] (Conselho da União Europeia, 2016b) que prevê «regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública» (*idem,* artigo 1.º, n.º1). Contudo, este documento legal, além de não se focar na ferramenta de Big Data, mencionando apenas conceitos intimamente conexos ao tema, como «partilha de informação» e «tomada de decisões automatizadas», não é específico quanto à forma como a técnica se pode materializar no âmbito do policiamento. Ou seja, os critérios sobre como usar os dados, quem pode usá-los, de que forma, como deve operar a partilha destes e que conclusões podem ser retiradas, são ainda indefinidos.

No contexto específico do policiamento e aplicação da lei, não existe um enquadramento legal claro acerca do uso ético do Big Data (Babuta, 2017, p. 36). Em Portugal, atualmente (2020) é desconhecida a existência de um documento legal que defina a aplicação de técnicas de Big Data. Até ao momento, o enquadramento jurídico existente com conexão com o tema reflete-se em duas estruturas legais diferentes que regulamentam as atividades policiais nacionais. Nomeadamente, o que vigora no artigo 272.º n.º 3 da Constituição da República Portuguesa (Canotilho & Moreira, 2005) que estabelece que *a prevenção dos crimes (...) só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos*. Adicionalmente, o artigo 2.º da Lei de Segurança Interna n. º 53/2008 de 29 de agosto estabelece que *a atividade de segurança interna pauta-se pela observância dos princípios do Estado de direito democrático, dos direitos, liberdades e garantias e das regras gerais de polícia*. Portanto, em Portugal, o contexto legal definido atualmente não permite atividades policiais que se materializem num controlo da população por via da monitorização individual. Visa-se, assim, garantir a defesa da integridade e privacidade da pessoa.

Desta forma, verifica-se um vazio legal que equaciona questões, na busca de respostas que possam ser equilibradas com o respeito pelos direitos humanos. Estudos anteriores denotam que os profissionais de investigação criminal também percecionam esta lacuna legislativa e a perspetivam como um entrave à aplicação ética do Big Data (Babuta, 2017; Chan & Moses, 2017; Neiva, 2020a, 2020b). Não obstante, denotam-se esforços legislativos no sentido de contornar

(10) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Conselho da União Europeia, 2016b). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680 (consultada a 8 de abril de 2020).

a inevitabilidade da evolução tecnológica, de forma a adequá-la a um contexto social democrático, minimizando as possibilidades de lesar direitos humanos.

Conclusão

Os esforços governamentais têm-se centrado no desenvolvimento de técnicas sofisticadas de combate ao crime, de gestão de riscos e de proteção da segurança, elevada a bem coletivo supremo. No entanto, com o aumento exponencial da implementação de ferramentas tecnológicas de luta contra ameaças criminais, verifica-se uma expansão incontrolável da vigilância e do controlo sobre os cidadãos. As técnicas de Big Data têm sido amplamente apoiadas para expandirem as malhas da vigilância no campo do policiamento e controlo da criminalidade. Com base neste contexto, este capítulo almejou refletir sobre as suas implicações ético-sociais e legais, focando a ideia de «composição da vigilância» (Haggerty & Ericson, 2000, p. 606). O foco de análise do presente texto explorou a relação entre vigilância, tecnologia, sociedade e lei, permitindo refletir sobre o controlo social e as desigualdades sociais, estratégias de discriminação populacional (Hier, 2003; Skinner, 2013, 2018a, 2018b) e impactos diversos na esfera dos direitos humanos.

Conforme discutido, há uma ênfase em torno das potencialidades tecnológicas do Big Data ao serviço do policiamento. Frequentemente surge descrito como útil na redução das taxas de criminalidade por nortear decisões e ações de justiça criminal que se baseiam em volumes de dados diversos, no entanto, a sua utilização suscita questões particulares. Desde logo, os dispositivos de Big Data possibilitam uma extensão das tradicionais técnicas de vigilância policial, recaindo sobre camadas sociais e grupos populacionais considerados suspeitos ou perigosos para sociedade. Desta forma, direcionam uma vigilância hierárquica, porque cria franjas populacionais distintas. No entanto, outra questão paradoxal que aparentemente pode parecer contraditória, é o facto das técnicas de Big Data se caracterizarem por serem rizomáticas (Haggerty & Ericson, 2000). Ou seja, por integrar várias áreas da vida quotidiana, materializam-se numa vigilância dispersa e descentralizada que recai sobre a globalidade da população. Esta ambivalência instiga a um debate ético-social e legal que deve superar as reflexões tradicionais sobre o tema.

A utilização do Big Data para realizar inferências, tendo por base dados policiais já recolhidos, potenciará a obtenção de correlações que (re)produzem consequências na sua execução. Nomeadamente, esta análise permitiu compreender de que forma é que uma vigilância policial norteada por sistemas

tecnológicos, como as estratégias de Big Data, pode potenciar o controlo sobre comunidades específicas já consideradas suspeitas num circuito fechado de vigilância (Williams & Johnson, 2004). Nomeadamente, (re)produzir desigualdades sociais, exacerbando a exclusão e criminalização de grupos considerados «de risco» na esfera do controlo social (Machado *et al.,* 2020). Processos de decisão algorítmica podem consolidar os preconceitos discriminatórios pré-existentes (Skinner, 2018a, 2018b), agudizando erros generalizados que persistem na sociedade, intensificando regimes descendentes de vigilância (Hier, 2003). Esta descendência vigilante é acentuada por via do aumento da distância entre quem vigia e os vigiados, reforçando as fragilidades sociais já existentes, ao mesmo tempo que oculta estas assimetrias por via de um discurso de imparcialidade e objetividade (Mantello, 2016).

Saliente-se, também, que o campo do policiamento e da segurança é um contexto particular desenvolvido muito antes da expansão dos dispositivos de Big Data. Portanto, muitos dos dados que norteiam as suas ações ainda não foram digitalizados, dependendo de estratégias tradicionais de vigilância para se materializarem. Apesar de a nível europeu, a utilização do Big Data na investigação criminal ser escassa (Neiva, 2020a, 2020b), este capítulo sugere que é crucial que se questionem as formas de análise e compreensão das correlações obtidas por via das suas ferramentas digitais e tecnológicas. A um nível prático, é um desafio a forma como poderá auxiliar a aplicação da lei no contexto do policiamento atual. Os estudos têm vindo a referir que não existem referências conclusivas que permitam afirmar que o uso deste tipo de tecnologias no policiamento reduza as taxas de crime (Mantello, 2016).

Ainda se refletiu acerca de que, enquanto fenómeno social, a técnica de Big Data reflete as estruturas sociais existentes, espelhando preconceitos policiais históricos, sociais e culturais. Imbuído num contexto social que é preciso compreender, as tecnologias não equacionam respostas para problemáticas sociais, a sua interpretação é que pode gerar novos conhecimentos. O processo de definição dos dados a recolher, a forma de os analisar, a decisão de com quem os partilhar e de que forma estes auxiliam as tomadas de decisões são questões cruciais e de reflexão sociológica urgente. Desta forma, é necessário refletir sobre o tipo de correlações que são obtidas, o seu nível de precisão, a sua utilidade e o seu uso para tomada de decisões no âmbito da governabilidade do crime. Por isso, é fundamental que este debate emerja e se compreendam as questões éticas, sociais e legais acerca do rumo que as estratégias de Big Data podem tomar. Compreender este mecanismo é crucial para aceder à forma como as análises de grandes dados podem conter enviesamentos.

Por fim, também se discutiu o modo como o desenvolvimento tecnológico nas estratégias de vigilância e controlo social supera, em larga escala, as respostas legais existentes. A um nível prático, é uma incógnita a forma como o policiamento deve implementar as estratégias de Big Data. Todo o processo de recolha, análise, processamento e partilha de dados carece de critérios legais definidos que norteiem este tipo de análise. Enquanto não se balizar a ética nestes processos, os direitos humanos e as liberdades fundamentais poderão colidir com este tipo de recolha, análise e partilha de dados no âmbito do policiamento (Babuta, 2017; Neiva, 2020a, 2020b).

Este capítulo visa incitar um debate público capaz de assumir um papel ativo na compreensão do desenvolvimento da tecnologia e dos seus limites. Estudos sobre outras formas tecnológicas de vigilância, por exemplo, acerca da implementação de circuitos de câmaras videovigilância no Reino Unido (ver Goold *et al.,* 2013) revelam que a inserção deste tipo de vigilância nas ruas tornou-se uma prática banal, um objeto de segurança aceite por todos como sendo parte integrante da vida pública. Este tipo de posicionamento face à expansão das tecnologias da vigilância deve alertar-nos para a possibilidade de a implementação e expansão das técnicas de Big Data puderem seguir o mesmo caminho, através da apatia e do silêncio social. Portanto, é crucial questionar «quão bons são os dados de vigilância e os modos de análise?» (Lyon, 2014, p. 9), debatendo o modo como Big Data é adotado como mecanismo de vigilância pelas agências policiais e securitárias.

Bibliografia

Andrejevic, M., & Gates, K. (2014). Big Data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185-196. http://www.surveillance-and-society.org

Assembleia Geral da Organização das Nações Unidas (1948). *Declaração Universal dos Direitos Humanos* (217 [III] A). Paris. https://www.un.org/en/universal-declaration-human-rights/

Assembleia Geral da Organização das Nações Unidas (1966). Pacto Internacional dos Direitos Civis e Políticos (2200 A [XXI]). Paris. https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

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*, 1-41. https://www.rusi.org/

Ball, K., Di Domenico, M., & Nunan, D. (2016). Big Data surveillance and the body-subject. *Body & Society, 22*(2), 58-81. https://doi.org/10.1177%2F1357034X15624973

Bauman, Z., Didier B., Paulo E., Elspeth G., Vivienne J., David L., & R.B.J. Walker. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121-144. https://doi.org/10.1111/ips.12048

Becker, H. (1963). *Outsiders – Studies in the sociology of deviance*. The Free Press.

Beckett, K., Kris N., Lori P., & Melissa, B. (2005). Drug use, drug possession arrests, and the question of race: Lessons from seattle. *Social Problems, 52*(3), 419-441. https://doi.org/10.1525/sp.2005.52.3.419

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

Boyd, D., & Crawford, K. (2012). Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662-679. https://doi.org/10.1080/1369118X.2012.678878

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

Canotilho, G., & Moreira, V. (2005). *Constituição da República Portuguesa. Lei do Tribunal Constitucional*. Coimbra Editora.

Chan, J., & Moses, L. (2016). Is Big Data challenging criminology? *Theoretical Criminology*, *20*(1), 21-39. https://doi.org/10.1177%2F1362480615586614

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

Christin, A. (2016). From daguerreotypes to algorithms: Machines, expertise, and three forms of objectivity. *ACM SIGCAS Computers and Society*, *46*(1), 27-32. https://doi.org/10.1145/2908216.2908220

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

Coll, S. (2014). Power, knowledge, and the subjects of privacy: Understanding privacy as the ally of surveillance. *Information, Communication & Society, 17*(10), 1250-1263. https://doi.org/10.1080/1369118X.2014.918636

Conselho da União Europeia (2016a). *Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE*. Jornal Oficial da União Europeia. http://data.europa.eu/eli/reg/2016/679/oj.

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

Cukier, K., & 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. https://heinonline.org/HOL/LandingPage?handle=hein.journals/fora92&div=46&id=&page=

Degli Esposti, S. (2014). When Big Data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, *12*(2), 209-225. https://doi.org/10.24908/ss.v12i2.5113

Drewer, D., & Miladinova, V. (2017). The Big Data challenge: Impact and opportunity of large quantities of information under the Europol regulation. *Computer Law & Security Review, 33*(3), 298-308. https://doi.org/10.1016/j.clsr.2017.03.006

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

Fiske, J. (1998). Surveilling the city: Whiteness, the black man and democratic totalitarianism. *Theory, Culture & Society, 15*(2), 67-88. https://doi.org/10.1177%2F026327698015002003

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Vintage

Giddens, A. (1990) *The consequences of modernity*. Polity Press.

Goold, B., Loader, I., & Thumala, A. (2013). The banality of security: The curious case of surveillance cameras. *British Journal of Criminology*, *53*(6), 977-96. https://doi.org/10.1093/bjc/azt044

Gonçalves, M. (2017). The EU data protection reform and the challenges of Big Data: Remaining uncertainties and ways forward. *Information & Communications Technology Law*, *26*(2), 90-115. https://doi.org/10.1080/13600834.2017.1295838

Haggerty, K. (2006). Tear down the walls: On demolishing the panopticon. In L. David (Ed.), *Theorizing surveillance. The panopticon and beyond* (2nd ed., pp. 37-59). Willan.

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

Halford, S., & Savage, M. (2017). Speaking sociologically with Big Data: Symphonic social science and the future for Big Data research. *Sociology*, *51*(6), 1132-1148. https://doi.org/10.1177%2F0038038517698639

Herschel, R., & Miori, V. (2017). Ethics & Big Data. *Technology in Society*, *49*, 31-36. https://doi.org/10.1016/j.techsoc.2017.03.003

Hier, S. (2003). Probing the surveillant assemblage: On the dialectics of surveillance practices as processes of social control. *Surveillance & Society*, *1*(3), 399-411. https://doi.org/10.24908/ss.v1i3.3347

Hu, M. (2015). Small data surveillance v. Big Data cybersurveillance. *Pepperdine Law Review, 42*(4), 773-844. https://heinonline.org/HOL/LandingPage?handle=hein.journals/pepplr42&div=28&id=&page=

Ikematu, R. S. (2001). Gestão de metadados: Sua evolução na tecnologia da informação. *DataGramaZero-Revista de Ciência da Informação*, *2*(6). https://brapci.inf.br/_repositorio/2010/01/pdf_0a6da12dc0_0007454.pdf

Innes, M. (2001). Control creep. *Sociological Research Online*, *6*(3), 13-18. https://doi.org/10.5153%2Fsro.634

Jahanian, F. (2014). The policy infrastructure for Big Data: From data to knowledge to action. *ISJLP: Journal of Law and Policy For The Information Society*, *10*(3), 865-880. https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc10&div=34&id=&page=

Joh, E. (2014). Policing by numbers: Big Data and the Fourth Amendment. *Washington Law Review*, *89*(1), 35-68. https://heinonline.org/HOL/LandingPage?handle=hein.journals/washlr89&div=5&id=&page=

Joh, E. (2017). Feeding the machine: Policing, crime data, & algorithms. *William. & Mary Bill of Rights Journal*, *26*(2), 287-302. https://heinonline.org/HOL/LandingPage?handle=hein.journals/wmbrts26&div=13&id=&page=

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*, *1*(1), 1-12. https://doi.org/10.1177%2F2053951714528481

Koper, C., Lum, C., & Willis, J. (2014). Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and

behaviourial aspects of implementing police technologies. *Policing*, *8*(2), 212-221. https://doi.org/10.1093/police/pau015

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%2F2053951717736338

Kuhn, T. (2012). *The structure of scientific revolutions* (4th ed.). University of Chicago Press.

Lei 53/2008. *Aprova a Lei de Segurança Interna*. Procuradoria-Geral Distrital de Lisboa, 29 de agosto. http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1012&tabela=leis

Lemert, E. (1967). *Human deviance, social problems, and social control*. University of Michigan.

Linder, T. (2019). Surveillance capitalism and platform policing: The surveillant assemblage-as-a-Service. *Surveillance & Society, 17*(1/2), 76-82. https://doi.org/10.24908/ss.v17i1/2.12903

Lyon, D. (1992). The new surveillance: Electronic technologies and the maximum security society. *Crime, Law and Social Change, 18*(1-2), 159-175. https://link.springer.com/content/pdf/10.1007/BF00230629.pdf

Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology, 19*(2), 135-149. https://doi.org/10.1177%2F0268580904042897

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 1-13. https://doi.org/10.1177%2F2053951714541861

Lupton, D., & Michael, M. (2017). «Depends on who's got the data»: Public understandings of personal digital dataveillance. *Surveillance & Society*, *15*(2), 254-268. https://doi.org/10.24908/ss.v15i2.6332

Machado, H., Granja, R., & Amelung, N. (2020). Constructing suspicion through forensic DNA databases in the EU. The views of the Prüm professionals. *The British Journal of Criminology*, *60*(1), 141-159. https://doi.org/10.1093/bjc/azz057

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, *6*(2), 1-11. https://doi.org/10.1177%2F2053951719895805

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, *16*(2), 219-237. https://doi.org/10.24908/ss.v16i2.8346

Mantelero, A. (2017). Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review*, *33*(5), 584-602. https://doi.org/10.1016/j.clsr.2017.05.011

Mantello, P. (2016). The machine that ate bad people: The ontopolitics of the precrime assemblage. *Big Data & Society*, *3*(2), 1-11. https://doi.org/10.1177%2F2053951716682538

Marx, G. (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

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

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, *4*(1), 1-7. https://doi.org/10.1177%2F2053951716686994

Metcalf, J., & Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society*, *3*(1), 1-14. https://doi.org/10.1177%2F2053951716650211

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 1-21. https://doi.org/10.1177%2F2053951716679679

Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing and Society*, *28*(7), 806-822. https://doi.org/10.1080/10439463.2016.1253695

Neiva, L. (2020a). O direito à privacidade no tempo do Big Data – Narrativas profissionais na União Europeia. *Revista Tecnologia e Sociedade, 16*(45), 1-20. http://dx.doi.org/10.3895/rts.v16n45.11439

Neiva, L. (2020b). *Big Data na investigação criminal: Desafios e expectativas na União Europeia*. Editora Húmus.

Pantazis, C., & Pemberton, S. (2009). From the «old» to the «new» suspect community: Examining the impacts of recent UK counter-terrorist legislation. *British Journal of Criminology*, *49*(5), 646-666. https://doi.org/10.1093/bjc/azp031

Pereira, M. (2019). *Big Data: O caso do sistema estratégico de informação, gestão e controlo operacional da Polícia de Segurança Pública* [Dissertação de Mestrado Integrado em Ciências Policiais, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa]. Repositório Comum. http://hdl.handle.net/10400.26/30342

Quijano-Sánchez L., & Camacho-Collados M. (2018). Applications of data science in policing: VeriPol an investigation support tool. *European Law Enforcement Resolution Bulletim, 1*(4), 89-96. http://91.82.159.234/index.php/bulletin/article/view/328

Raley, R. (2013). Dataveillance and countervailance. In L. Gitelman (Ed.), *Raw data is an oxymoron* (pp. 121-145). MIT Press.

Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online, 94*(15), 15-50. https://heinonline.org/HOL/LandingPage?handle=hein.journals/nyulro94&div=3&id=&page=

Ridgeway, G. (2018). Policing in the era of Big Data. *Annual Review of Criminology*, *1*, 401-419. https://doi.org/10.1146/annurev-criminol-062217-114209

Sanders, C., Weston, C., & Schott, N. (2015). Police innovations, «secret squirrels» and accountability: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology*, *55*(4), 711-729. https://doi.org/10.1093/bjc/azv008

Skinner, D. (2013). «The NDNAD has no ability in itself to be discriminatory»: Ethnicity and the governance of the UK national DNA database. *Sociology*, *47*(5), 976-992. https://doi.org/10.1177%2F0038038513493539

Skinner, D. (2018a). Race, racism and identification in the era of technosecurity. *Science as Culture*, *29*(1), 77-99. https://doi.org/10.1080/09505431.2018.1523887

Skinner, D. (2018b). Forensic genetics and the prediction of race: What is the problem?. *BioSocieties*, *15,* 329-349. https://doi.org/10.1057/s41292-018-0141-0

Uprichard, E. (2013, 1 de outubro). Focus: Big Data, little questions? *Discover Society*. http://discoversociety.org/wp-content/uploads/2013/10/DS_Big-Data.pdf

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208. https://doi.org/10.24908/ss.v12i2.4776