U.PORTO

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

As perspetivas dos polícias sobre a aplicação do *big data* no policiamento

Carolina Gomes Glória

M

2024

FACULDADE DE **DIREITO**

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para obtenção do Grau de Mestre em Criminologia, elaborada sob orientação da Professora Doutora Carla Sofia de Freitas Lino Pinto Cardoso.

Declaração de Integridade

Declaro ter atuado com integridade na elaboração da presente dissertação de mestrado, não recorrendo à prática de plágio ou a qualquer forma de falsificação dos resultados apresentados.

Universidade do Porto, 21 de julho de 2024,

Carolina Gomes Glória

Dedico este trabalho à minha luz, os meus pais.

Agradecimentos

À Professora Doutora Carla Cardoso, pela sua compreensão nos momentos mais difíceis e pelo seu cuidado ao longo de todo este processo. Por me orientar nos momentos de dúvida.

Aos meus pais, que são a minha luz e que dedicam as suas vidas a mim e à minha irmã. Tudo o que é meu é vosso. Para sempre.

À minha irmã, que é o meu tesouro.

À minha avó, que é o meu exemplo. Pelo seu coração gigante e pelo seu amor incondicional por mim. Amo-te para lá desta vida.

À minha madrinha, por ser a minha guia. Por me lembrar do meu valor e que o caminho é sempre para a frente. Por me lembrar que no nosso coração só cabem coisas boas e ser a calmaria nos dias mais turbulentos.

À Polícia de Segurança Pública, especialmente aos agentes entrevistados, pela disponibilidade e simpatia com que me receberam. Pela prontidão com que aceitaram participar nesta viagem. A vós, bem hajam.

A todos os professores que me acompanharam durante o meu percurso académico, pela excelência e pelo rigor. Pela qualidade que vos distingue.

Às minhas queridas amigas Carla e Inês, por me apoiarem e por me ouvirem. Por serem aquela voz amiga. Espero retribuir-vos tudo o que fizeram por mim.

À Clara, a melhor colega de trabalho do mundo, pela sensibilidade e pela gentileza. Pelos sentimentos nobres que nutre por mim e pela minha mãe. Por ter o coração no sítio certo.

A todos os que contribuíram para esta aventura. Bem hajam.

Resumo

A literatura científica aponta o papel promissor do uso do *big data* no policiamento, enquanto ferramenta que permite conhecer a criminalidade, contextos, padrões, *modus operandi*, ofensores e redes criminais e o direcionamento mais eficaz dos recursos técnicos e humanos existentes, potenciando uma melhor investigação dos crimes, modelos de policiamento dirigidos a problemas (e.g. *hot spots*), a prevenção do crime e o que muitos autores chamam *predictive policing*.

Os estudos apresentam o valor positivo do *big data* na redução da criminalidade como largamente reconhecido pela comunidade científica, propondo-se uma introdução gradual e destemida do mesmo.

No entanto, os autores identificam também alguns desafios que o uso do *big data* no policiamento pode suscitar, nomeadamente no que respeita às questões éticas, legais e sociais que prejudicam a confiança dos cidadãos na polícia.

Deste modo, para responder à escassez de estudos portugueses sobre esta matéria e para procurar conhecer a realidade da polícia portuguesa quanto ao uso do *big data*, o presente trabalho tem como objetivo aceder às perceções, opiniões e expectativas dos polícias sobre o uso desta ferramenta no policiamento. Mais especificamente, procura-se perceber quais as vantagens e os desafios que os polícias encontram nas atividades da polícia no seu quotidiano durante o uso do *big data*, quer na prevenção como na investigação criminal.

Assim, com base numa metodologia qualitativa e na análise de entrevistas realizadas a estes profissionais, os resultados permitem explorar os benefícios e os riscos da sua utilização pela polícia, contribuindo para o debate contemporâneo, e equacionar pistas sobre as necessidades que devem ser atendidas no futuro para um uso mais profícuo do *big data* na prevenção e investigação criminal.

Palavras-chave: *big data*, policiamento preditivo, eficácia e eficiência, desafios éticos, legais e sociais

Abstract

Scientific literature points to the promising role of using big data in policing, as a tool that allows understanding crime, contexts, patterns, modus operandi, offenders and criminal networks and the most effective targeting of existing technical and human resources, enhancing better investigation of crimes, problem-driven policing models (e.g., hot spots), crime prevention, and what many authors call predictive policing.

The studies present the positive value of big data in reducing crime as widely recognized by the scientific community, proposing its gradual and fearless introduction.

However, the authors also identified some challenges that the use of big data in policing can raise, particularly with regard to ethical, legal and social issues that undermine citizens' trust in the police.

Therefore, to respond to the lack of Portuguese studies on this matter and to seek to understand the reality of the Portuguese police regarding the use of big data, the present work aims to reach the perceptions, opinions and expectations of police officers regarding the use of this tool in the policing. More specifically, try to understand the advantages and challenges that police encounter in their daily police activities when using big data, both in prevention and in criminal investigation.

Thus, based on a qualitative analysis and the analysis of interviews carried out with these professionals, the results allow us to explore the benefits and risks of its use by the police, contributing to the contemporary debate, and to consider clues about the needs that must be met in the future. for a more fruitful use of big data in criminal prevention and investigation.

Keywords: big data, predictive policing, effectiveness and efficiency, ethical, legal and social challenges

Índice

Introdução

A presente dissertação, desenvolvida no âmbito do Mestrado em Criminologia da Faculdade de Direito da Universidade do Porto, tem como objetivo primordial contribuir para a literatura científica com uma investigação sobre as perceções, opiniões e expetativas dos polícias sobre o uso do *big data* na prevenção e investigação criminal.

Ainda que sejam apresentadas várias definições de *big data* na literatura científica (Brayne, 2017), os seus contributos positivos para o policiamento são amplamente reconhecidos pela comunidade científica.

Esta ferramenta, que é uma consequência da era de *datafication*[1] que atravessamos, parece maximizar a eficácia da polícia, quer na prevenção quer na investigação criminal, isto porque pode permitir conhecer a realidade antes de intervir (Ylijoki & Porras, 2016).

Deste modo, para Neiva (2021), o *big data* é uma grande quantidade de dados que provém de diversas fontes, cujo processamento e análise permite conhecer as causas dos problemas e identificar padrões e tendências nos dados, orientando os recursos técnicos e humanos disponíveis e as medidas táticas e estratégicas a serem implementadas.

A análise desta grande quantidade de dados necessita do uso de *softwares* avançados (Tsai et al., 2015) para que a informação obtida permita identificar quais os crimes que são mais cometidos, por quem são cometidos, onde são cometidos, quando são cometidos, como são cometidos e porque é que são cometidos e ainda detetar tendências criminais futuras.

No entanto, os estudos apontam que, frequentemente, é condicionado por questões práticas que prejudicam a eficácia da polícia na resposta às ameaças. Assim, de acordo Babuta (2017) e Chan e Moses (2017), os principais problemas apresentados relacionam-se com as fontes dos dados, os recursos tecnológicos existentes, a partilha de dados intra e interagências e com a formação dos analistas.

Não obstante, os estudos apontam também desafios éticos, legais e sociais que o uso indevido do *big data* pela polícia pode levantar, nomeadamente a discriminação de determinados grupos éticos e sociais e a violação de direitos fundamentais, como a liberdade individual, a igualdade perante a lei, a privacidade, o consentimento e presunção de inocência (Brayne, 2017; Neiva, Granja & Machado, 2022).

[1] *Datafication* é o processo de converter vários aspetos da vida em dados que podem ser analisados, a fim de orientar a tomada de decisões (Mejias & Couldry, 2019)

Assim, a fim de suprir a lacuna na investigação científica sobre esta matéria no contexto português, o presente estudo visa explorar o uso do *big data* no policiamento, procurando compreender os benefícios e riscos da sua utilização, identificados pelos polícias.

Esta dissertação divide-se em quatro grandes partes, correspondendo a primeira ao enquadramento teórico que articula conceitos teóricos e apresenta os principais achados da literatura científica sobre esta matéria.

A segunda parte será dedicada à apresentação da metodologia utilizada, com a identificação dos objetivos de estudo, das questões de investigação, da amostra, dos instrumentos utilizados para operacionalização das variáveis e procedimentos adotados para recolha e análise dos dados.

A terceira parte consistirá na análise temática dos dados recolhidos, bem como a apresentação dos resultados obtidos.

A última parte será dedica à discussão dos resultados, às limitações encontradas e direções futuras.

PARTE I – ENQUADRAMENTO TEÓRICO

1. A definição do objeto de estudo: *big data*

Diariamente, milhões de dados são gerados durante as atividades do nosso quotidiano (Ylijoki & Porras, 2016). As nossas informações pessoais e comportamentos são transformados em dados numéricos que alimentam algoritmos e permitem prever fenómenos futuros. Estes grandes conjuntos de dados variados permitem às instituições conhecerem a sociedade e orientarem as suas decisões consoante as previsões produzidas (Ylijoki & Porras, 2016; Zakir et al., 2015).

Deste modo, as intervenções das instituições na sociedade são estratégicas, na medida em que resultam de uma ponderação face ao conhecimento obtido dos dados. Ao identificarem tendências e padrões, as decisões tomadas pelas instituições direcionam-se às causas dos problemas, tornando a sua intervenção mais eficaz (Ali, 2015).

À grande quantidade de dados gerados por diversas fontes presentes no nosso quotidiano, designamos *big data*, os quais são processados e analisados com o objetivo de orientar/informar a tomada de decisões (Ali, 2015; Zakir et al., 2015).

Além disso, o processamento e análise dos dados brutos ocorre de forma rápida e em tempo real, ou seja, a produção de conhecimento com base nos dados é quase instantânea.

Deste modo, o uso do *big data* está relacionado ao uso de *softwares* avançados que permitem um amplo cruzamento dos dados variados e uma análise e processamento dos mesmos praticamente imediata (Tsai et al., 2015). Além disso, atualmente, a inteligência artificial e o *data mining*[2] permitem ao aprender com os dados, tornar os sistemas cada vez mais inteligentes na deteção de padrões e mais eficazes nas previsões (L´heureux et al., 2017). A introdução de dados no sistema permite uma aprendizagem contínua do algoritmo, à semelhança do que acontece com a inteligência humana (Cozman, 2020). Contudo, a principal diferença entre a inteligência artificial e a inteligência humana é o volume de dados que são processados, tornando as máquinas essenciais para o uso eficaz do *big data*.

Pelas suas potencialidades na produção de dados que orientam estratégias eficazes, Bartlett et al. (2018) apontaram o *big data* como a ferramenta de pesquisa mais importante do século XXI. No entanto, não há uma definição universal do termo na literatura científica, apresentando-se milhares de conceptualizações. Por exemplo, os autores Favaretto et al. (2019), definiram *big data* nos seus trabalhos como um volume extenso de dados que são

[2] O *data mining* consiste num conjunto de ferramentas sofisticadas que permitem aos analistas identificar padrões e tendências nos dados para resolver problemas por meio da análise dos mesmos (Fouché & Langit, 2011; Tsai et al., 2015).

recolhidos, analisados, convertidos em algoritmos, categorizados numericamente e identificados por um índice com o objetivo de extrair informação que informe/oriente.

No mesmo sentido, para Babuta (2017), *big data* corresponde a um grande conjunto de dados que são tratados para produzir um produto que permite orientar a tomada de decisões. Contudo, a grande quantidade de dados pressupõe o uso de *softwares* avançados, uma vez que a utilização dos métodos tradicionais condiciona o alcance dos resultados obtidos (Babuta, 2017; Tsai et al., 2015).

Já Boyd & Crawford (2012) apresentam o conceito de uma forma diferente. Para os autores, esta ferramenta resulta da interação de três elementos: (i) a tecnologia, visto que resulta e usufrui do poder tecnológico; (ii) a análise, uma vez que esta permite deteção de padrões e tendências, e (iii) a mitologia, já que assenta na ideia de que uma maior quantidade de dados resulta num maior conhecimento da realidade.

Também Ridgeway (2018) apresentou três aspetos que definem o *big data:* (i) volume: grandes conjuntos de dados que devem ser processados e analisados através de *softwares* avançados, visto que os métodos tradicionais (análise humana) condicionam o alcance dos resultados obtidos. Por exemplo, segundo Eberendu (2016), o número de indivíduos que realizam chamadas, enviam mensagens e utilizam as redes sociais já ultrapassa os 5 biliões, em todo o mundo, o que resulta num volume de dados, cujo o armazenamento, o processamento e a análise excede os limites dos métodos tradicionais; (ii) velocidade: com o apoio do poder tecnológico, uma grande quantidade de dados pode ser processada e analisada rapidamente e em tempo real, gerando um produto que orienta e informa, (iii) variedade: dado que a recolha de dados assenta em várias fontes distintas, os dados obtidos são variados. Esta variedade de fontes resulta também do desenvolvimento tecnológico, nomeadamente da possibilidade da recolha de dados sem a necessidade de uma relação de proximidade entre observador e observado, por exemplo, através de drones ou da pegada digital (Andrejevic & Gates, 2014; Eberendu, 2016)

Neste sentido, explorando a natureza dos dados, Neiva (2019) identifica três tipos de fontes, nomeadamente as dirigidas, as automatizadas e as voluntárias.

Nas fontes dirigidas, os dados resultam de uma recolha direcionada consoante as necessidades. Neste tipo de fontes podemos incluir os questionários ou as entrevistas, dado que são métodos em que se procura respostas a perguntas predefinidas. Embora nestas fontes haja um maior controlo sobre os dados, continuam a existir enviesamentos e limitações que podem resultar, por exemplo, da forma como as perguntas são formuladas (Alshenqeeti, 2014).

Já nas fontes automatizadas, a recolha de dados ocorre automaticamente por sistemas tecnológicos, sem que seja necessária a intervenção humana direta. Neste tipo de fontes podemos considerar, por exemplo, os dados de navegação na *internet*. Estas fontes tendem a gerar milhões de dados em tempo real, alimentando as bases de dados, mas encontram desafios éticos, nomeadamente no que respeita ao direto à privacidade (Schermer, 2011), sob os quais é necessário refletir.

Por sua vez, nas fontes voluntárias, os dados são fornecidos voluntariamente pelos indivíduos, sem que haja necessariamente uma compensação direta. Aqui podemos incluir os comentários nas redes sociais ou as avaliações de produtos, por exemplo. Estes dados, ainda que forneçam uma ideia geral sobre as preferências e opiniões dos indivíduos, também podem ser afetados por enviesamentos e levantar questões quanto à sua veracidade e validade (Burcher & Whelan, 2018; Schermer, 2011), sendo essencial que a sua inserção no sistema de dados da polícia seja precedida por um procedimento de validação (Sanders & Sheptycki, 2017)

Assim, cada tipo de fonte de dados possui as suas próprias vantagens e desafios, sendo que a escolha dependerá dos objetivos da recolha, da disponibilidade de recursos e de outras considerações contextuais. No entanto, o cruzamento de dados provenientes de várias fontes de informação é uma prática importante para a validação das informações recolhidas, pois permite a deteção de erros e o enriquecimento dos dados (Chi, 2019).

1.1. *Big data* e *intelligence*

Frequentemente, os conceitos de dados, informação e conhecimento são utilizados indevidamente como sinónimos, sendo que Rowley (2007) distingue-os da seguinte forma: os dados não possuem significado e baseiam-se em meras descrições objetivas; a informação resulta da interpretação dos dados, de modo a representar uma realidade; e o conhecimento é a combinação da informação organizada e processada, que origina o produto *intelligence.*

O produto *intelligence* é designado por Scott (2000) como o conhecimento especializado que é usado pela polícia para identificar quem está a cometer crimes, qual o *modus operandi*, onde são os *hot spots*, quando é que os crimes são cometidos e quais são as razões para cometerem esses crimes.

Neste sentido, Peterson (2005) apresenta quatro finalidades do produto *intelligence*, nomeadamente a estratégica, que fornece uma imagem macro, de longo prazo, de tendências e previsões para o futuro, usada para o planeamento, definição de prioridades e alocação de recursos; a tática, que orienta a ação, a curto prazo, relacionada com investigações

específicas; a centrada em alvos estratégicos, que identifica e descreve as organizações/ofensores mais problemáticos para orientar operações contra estes; e a focada em perfis de problemas, que identifica e descreve tipos de crime ou *hot spots* de crimes emergentes.

Este produto *intelligence* é gerado em centros especializados dentro das organizações da polícia que se organizam em 3 níveis, consoante as suas responsabilidades. Assim, o nível 1, dedica-se aos crimes que têm um impacto local; o nível 2, centra-se nos crimes transfronteiriços que afetam mais do que uma unidade da polícia; e o nível 3, direciona-se aos crimes nacionais e internacionais (Cope, 2004)

Não obstante a organização apresentada por Cope (2004), é essencial que exista uma interconexão dos três níveis, através do compartilhamento de dados, visto que, por exemplo, o conhecimento produzido por uma unidade local da polícia pode permitir que uma agência europeia localize um ofensor que é alvo de mandado de captura internacional.

Dada a importância da *intelligence* para o melhoramento do policiamento, a *International Association of Chiefs of Police* organizou uma cúpula com mais de 100 especialistas em *intelligence* que concluíram que era essencial promover o policiamento baseado em *intelligence* para proteger os direitos fundamentais dos cidadãos e fortalecer os laços de confiança entre polícias e cidadãos, procurando colmatar os défices analíticos e de informação e investindo na formação dos analistas em tecnologia (Peterson, 2005).

Esta cúpula fundou também o *Global Intelligence Working Group*, composto por cerca de 30 profissionais de *intelligence*, que desenvolveu o *National Criminal Intelligence Sharing Plan*[3], aprovado pelo Procurador-Geral dos Estados Unidos, em outubro de 2003 (Bureau of Justice Assistance, 2003).

O *National Criminal Intelligence Sharing Plan* propõe que o funcionamento da *intelligence* é cíclico e que se divide em seis fases, mais especificamente, o planeamento, a recolha, o processamento, a análise, a disseminação e o *feedback* (Fuentes, 2006; Walsh, 2011)

O planeamento consiste no primeiro momento do ciclo e ocorre antes da recolha dos dados. Esta etapa visa apurar as necessidades de recolha para garantir que os dados obtidos preenchem as lacunas do sistema. Note-se que um bom planeamento das necessidades permite uma recolha mais produtiva.

Além disso, é também importante a coordenação dos métodos e a proibição de métodos ilegais na recolha (Richards, 2012).

[3] O *National Criminal Intelligence Sharing Plan* teve como objetivo combater as barreiras que impedem o compartilhamento de informações intra e interagências (Bureau of Justice Assistance, 2003).

A segunda etapa é a recolha, sendo que as formas mais utilizadas de recolha de dados são a vigilância física, vigilância eletrónica, informantes confidenciais, agentes encobertos, reportagens, *internet* e registos públicos (Peterson, 2005).

A terceira fase é o processamento que pretende avaliar e cruzar os dados e excluir aqueles que não são válidos e credíveis. Cada vez mais, há a introdução de novas tecnologias para agilizar este processo (Boyd & Crawford, 2012).

A quarta etapa é a análise. É aqui que ocorre a transformação dos dados brutos recolhidos em produto *intelligence*. É nesta fase que se identificam padrões de crime, nomeadamente ofensores, *hot spots*, *modus operandi* e causas do crime.

Não obstante, importa esclarecer que o analista não decide sobre as medidas a implementar. O analista somente sugere o que deve ser feito, sendo transmitida a responsabilidade do modo como se intervém aos líderes da polícia (Ratcliffe, 2003). Deste modo, a análise é um processo que se centra na sintetização dos dados, no desenvolvimento de inferências e proposta de recomendações.

A quinta etapa é a divulgação e é quando ocorre a comunicação, por meio de relatórios, do produto *intelligence* a quem precisa dela (Sanders et al., 2015). O produto *intelligence* deve ser partilhado consoante as necessidades das agências (Peterson, 2005).

Por fim, a sexta fase é o *feedback*. O relatório de divulgação do produto *intelligence* é acompanhado por um formulário destinado ao *feedback* sobre a relevância e utilidade do produto, por parte dos seus consumidores (Ratcliffe, 2008). Ou seja, há um momento de reavaliação para apurar o valor do produto *intelligence*.

Após a avaliação e apresentação de novas necessidades pelos consumidores, reinicia-se o ciclo (Morelato et al., 2013).

No entanto, Burcher & Whelan (2018) apresentam críticas ao modelo de funcionamento da *intelligence* proposto pelo *National Criminal Intelligence Sharing Plan*, uma vez que este modelo não refere o papel orientador que produto *intelligence* assume para as decisões dos líderes e a produção da *intelligence* parece ser mais fluída na prática do que na teoria.

Por sua vez, Ratcliffe (2003) sugere que o funcionamento da *intelligence* ocorre numa dinâmica triangular, em que os vértices apresentam as três componentes base do processamento, nomeadamente o ambiente criminal, a análise e o decisor, e os lados representam os processos que permitem a conexão dessas componentes, designadamente a interpretação, influência e o impacto (Walsh, 2011).

O modelo de funcionamento da *intelligence* proposto por Ratcliffe (2003) aponta a necessidade da recolha de dados do ambiente criminal para a sua interpretação. A análise

dos dados brutos recolhidos é essencial para identificar as causas dos crimes, ofensores, *modus operandi*, *hot spots* e tendências futuras para que as medidas táticas e estratégicas implementadas pela polícia sejam eficazes para a prevenção e combate ao crime.

No entanto, para que as organizações da polícia possam adotar esta dinâmica triangular é necessário que os decisores entendam o valor do produto *intelligence* para que o considerem nas suas tomadas de decisões (Ratcliffe, 2008, Walsh, 2011; Fuentes, 2006). Deste modo, contrariamente ao modelo anterior, este modelo centra-se na importância do papel dos decisores para a implementação de medidas que permitam a prevenção e combate do crime.

1.2 *Big data* e inteligência artificial

Todas as nossas informações pessoais e comportamentos podem ser transformados em dados numéricos que permitem conhecer a criminalidade, contextos, padrões, *modus operandi*, ofensores e redes criminais e, consequentemente, uma alocação mais eficaz dos recursos técnicos e humanos existentes, potenciando uma melhor investigação dos crimes, modelos de policiamento dirigidos a problemas, prevenção do crime e o que muitos autores chamam *predictive policing* (Ali, 2015).

O *big data* é uma ferramenta essencial para o policiamento preditivo e para que os corpos de polícia no terreno tenham acesso a informação importante de imediato. Contudo, dada a importância do poder tecnológico para o processamento de uma grande quantidade de dados, é essencial compreender a relação desta ferramenta com a inteligência artificial, nomeadamente a influência que estas exercem uma sob a outra.

De acordo com Neto, Bonacelli & Pacheco (2020), a inteligência artificial é uma tecnologia avançada que visa o processamento de grandes conjuntos de dados para a produção de resultados, assemelhando-se à inteligência humana.

Por outras palavras, o objetivo é o processamento e análise de dados brutos a uma velocidade que excede a capacidade humana, mas que é essencial para auxiliar a tomada de decisões.

O Sistema de Inteligência Artificial encontra-se legalmente definido no Regulamento do Parlamento Europeu e do Conselho (2021) enquanto um "programa informático desenvolvido com uma ou várias das técnicas e abordagens (…), capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage".

No que respeita ao desenvolvimento da inteligência artificial, Lee (2018) caracteriza-o como gradual e constante, ainda que em determinados momentos temporais, tenham ocorrido

avanços significativos em áreas específicas. Estes picos evolutivos devem-se, essencialmente, às descobertas científicas e aos desenvolvimentos tecnológicos.

Ainda quanto ao seu desenvolvimento e funcionamento, existem três dimensões essenciais (Cozman,2020) , nomeadamente a representação do conhecimento, que é a capacidade da inteligência artificial em converter o conhecimento humano numa linguagem que é entendida pelos algoritmos e que permite o sistema tomar decisões (Bench-Capon, 1990); o processamento de linguagem natural, permite que o sistema analise dados textuais para a extração de informação útil (Taulli, 2019); e a aprendizagem da máquina, que permite que o sistema aprenda com a introdução de novos dados (Araújo et al., 2020). Esta aprendizagem contínua da máquina permite criar melhores previsões e a tomada de decisões mais eficazes. A capacidade de aprendizagem do sistema assemelha-se à capacidade de aprendizagem humana.

Note-se que esta última dimensão é muito importante quando pensamos no uso do *big data* pela polícia, isto porque, à medida que surgem cada vez mais dados, as previsões que daí resultam são, graças à inteligência artificial, mais eficazes, contribuindo para um policiamento com melhores resultados (L'heureux et al., 2017). Ou seja, se por um lado, o sistema necessita de novos dados para evoluir, sem a inteligência artificial o processamento e análise do *big data* parece condicionado.

Deste modo, a inteligência artificial é uma tecnologia poderosa para o Sistema de Justiça Criminal, dado o suporte que dá ao policiamento, contribuindo positivamente para a segurança pública. Por exemplo, Telles (2021) refere que a utilização da inteligência artificial pode aumentar a possibilidade de vigilância e controlo do espaço público pelas forças de segurança pública, através de tecnologias com funções de reconhecimento facial ou localização geográfica como os drones, sem que seja necessária a intervenção humana. A vigilância já não se baseia numa relação de proximidade entre observador e observado, uma vez que as novas tecnologias permitem que a polícia realize uma vigilância à distância.

Neste sentido, a preocupação em recolher grandes quantidades de dados para conhecer a realidade e intervir preventivamente e a contribuição da tecnologia para a construção de um policiamento mais eficaz, entre outros fatores contextuais, reforçaram a necessidade de mudança do paradigma de policiamento em vigor, surgindo assim no final do século XX, o *intelligence-led policing*, um modelo de policiamento que se baseia no produto *intelligence* para criar estratégias táticas e preventivas mais profícuas (Wiggett et al, 2002).

2. O valor dos dados para o combate à criminalidade

De acordo com Kent (1986), a análise do crime é importante, porque pode auxiliar os líderes na gestão de problemas como a criminalidade, através do conhecimento do crime e do planeamento estratégico e operacional. Assim, o produto *intelligence* produzido pelos analistas pode orientar as decisões dos líderes na prevenção e repressão criminal (Kent, 1986).

Neste sentido, na década de 90, a Polícia de *Kent* utilizou os contributos positivos da análise do crime para o combate à criminalidade, na medida em que a análise dos dados recolhidos, através da aplicação de inquéritos de delinquência autorrevelada, permitiu identificar que a maioria dos sujeitos cometem crimes pontualmente, sendo que a maior porção da criminalidade é da responsabilidade de um pequeno grupo de ofensores, denominados ofensores prolíficos (Ratcliffe, 2008).

Deste modo, a Polícia de *Kent* concentrou os recursos existentes nos ofensores prolíficos, o que permitiu uma redução da criminalidade (Hale et al., 2004), enfrentando-se o aumento acentuado das ofensas contra a propriedade, mesmo num período em que houve reduções orçamentais na polícia (Fernandes, 2014,).

A definição de prioridades e a estratégia de policiamento implementada pela Polícia de *Kent* permitiu uma queda de 24% da criminalidade, num período de 3 anos, algo que lhe concedeu notoriedade e encorajou a implementação do método noutros países (McGarrell et al.,2007; Ratcliffe, 2008), criando-se o *intelligence-led policin*g, que é definido por Fuentes (2006) como uma filosofia colaborativa que analisa os dados recolhidos para criar informações úteis, permitindo à polícia implementar as melhores estratégias preventivas e táticas e a alocação de recursos.

No entanto, existiram outros fatores contextuais que impulsionaram a mudança de paradigma como a globalização. A globalização decorreu a partir de meados de 1980 e permitiu a livre circulação de pessoas, bens e produtos entre os países da União Europeia e o desenvolvimento dos transportes terrestres, aéreos e marítimos e das Tecnologias de Informação e Comunicação (Bleur & Johnson, 2016; McGarrell et al., 2007).

Relativamente às Tecnologias de Informação e Comunicação, o seu desenvolvimento permitiu criar uma base de dados comum entre vários países europeus que dinamizava e facilitava a partilha de dados entre corpos policiais, alcançando-se um maior conhecimento do crime e contribuindo positivamente para a sua prevenção.

No entanto, existiram também algumas ameaças que resultaram desta união entre Estados, por exemplo a criação e expansão das redes criminais e ofensas globais como o terrorismo.

Assim, a globalização reforçou a necessidade de um policiamento preditivo para prevenir os danos graves causados por este tipo de ameaças (Peterson, 2005).

Deste modo, a globalização, as ameaças globais e o sucesso da Polícia de *Kent* permitiram a implementação do *intelligence-led policing*, que se centra num modelo em que estratégias táticas e preventivas aplicadas devem ser orientadas pelo produto *intelligence* (Bleur & Johnson, 2016; McGarrell et al, 2007)

Embora existam várias conceptualizações sobre o modelo, Ratcliffe (2008), um dos autores mais citados nesta matéria, apresenta-o como um modelo managerialista assente numa filosofia de gestão em que o produto *intelligence* é basilar para a tomada de decisões objetivas sobre a repressão e prevenção do crime, com base em estratégias preventivas e táticas. O produto *intelligence* resulta do processamento e análise dos dados recolhidos do meio e informa/orienta o policiamento, porque permite interpretar a realidade.

Para Carter (2004), o *intelligence-led policing* foca-se nas principais atividades criminosas, porque se se nos centrarmos na deteção dos criminosos mais graves, podemos reduzir significativamente o crime.

Uma das principais diferenças entre o *intelligence-led policing* e o modelo de polícia anterior é o foco na segurança proativa, na vigilância e na gestão do risco (Ericson & Haggerty, 1997). Dado o valor do produto *intelligence*, os líderes da polícia devem considerá-lo na tomada de decisões, tornando as estratégias adotadas mais eficazes. Esta ação da polícia orientada pela *intelligence* permite o melhoramento do policiamento.

Deste modo, o *intelligence-led policing* assenta em 7 princípios basilares, nomeadamente a proatividade e a prevenção, a eficiência e eficácia profissional, a tomada de decisão com base em dados, o uso de tecnologia, a cooperação e o compartilhamento de dados intra e interagências, a abordagem *top-down* e o custo-benefício.

Contrariamente ao que ocorria no modelo de polícia anterior, no *intelligence-led policing* a recolha ativa dos dados é essencial para a deteção de padrões e tendências e intervenção precoce no meio (Wiggett et al., 2002). Este modelo baseia-se num policiamento preditivo, em que há uma procura ativa de desvios para prevenir os danos.

A recolha de dados permite ainda a deteção das necessidades, permitindo uma melhor gestão dos recursos técnicos e humanos, potenciando a eficiência e eficácia profissional (Taylor e Russel, 2014). Assim, a alocação dos recursos, além de poder potenciar a eficácia, pode minimizar os custos.

Mais se acrescenta que a eficácia do policiamento está também relacionada com o reconhecimento do valor da *intelligence* pelos líderes da polícia. Os líderes da polícia devem

considerar o produto *intelligence* para que as medidas implementadas no meio para a prevenção e combate do crime sejam eficazes (Ratcliffe, 2003).

A importância do papel dos líderes da polícia destaca a abordagem *top-down* do modelo (Ratcliffe, 2003), ou seja, as medidas adotadas pela polícia no terreno estão sob dependência hierárquica das patentes mais altas.

Para que o produto *intelligence* seja útil é necessária a utilização de *softwares* avançados para o processamento e análise de grandes quantidades de dados pelos polícias (Tsai et al., 2015). O uso de tecnologias avançadas não somente permite o cruzamento de uma maior quantidade de dados como melhora a interpretação do crime.

No entanto, para a interpretação do crime, é também essencial o compartilhamento de dados intra e interagências, seja para testar a validade dos dados ou para combater ameaças globais (Cope, 2004).

O cumprimento dos princípios básicos do modelo permitem não somente a melhoria da eficiência e a eficácia das operações táticas e estratégicas da polícia, mas também promove uma abordagem mais proativa e preventiva na manutenção da segurança pública (Wiggett et al, 2002)

Os resultados positivos do uso do *intelligence-led policing* no combate ao crime organizado, especificamente nos cartéis de droga, foram apresentados por Ratcliffe e Guidetti (2008) num estudo de caso, designado Operação *Nine Connect*.

Este estudo, além de documentar a recolha e análise de dados, os seus resultados e as tomadas de decisão, descreve também o contributo das investigações lideradas pela *intelligence* na gestão da informação.

O estudo de Ratcliffe e Guidetti (2008) centra-se na Polícia de *New Jersey* e *da Federal Bureau* que realizaram investigações entre 2001 e 2004, e constataram a existência de um elevado número de gangues na cidade. No total, foram identificados 148 gangues, dos quais 28 eram constituídos por mais de 100 elementos. Note-se que estes grupos foram responsáveis por mais de 500 incidentes entre gangues nas escolas. Além disso, as investigações permitiram ainda identificar os três maiores e mais violentos gangues, nomeadamente os *Crips*, os *Latin Kingsm* e os *Bloods*.

Um ano depois, em 2005, realizou-se uma nova avaliação estratégica que definiu as quatro prioridades da ação da polícia: identificar, observar, infiltrar e desmantelar grupos de criminalidade organizada; identificar, observar, infiltrar e impedir o tráfico de drogas ilegais, o transporte e a sua distribuição dentro e fora do Estado; identificar, observar, infiltrar e erradicar os gangues mais violentos e assustadores dentro do Estado; fortalecer a aliança

entre a Polícia de *New Jersey* e a *Federal Bureau* em todas as áreas de investigação no combate ao terrorismo

Nesse mesmo ano, as investigações concluíram que os *Bloods* eram o gangue mais problemático e influente no que toca à distribuição e comercialização de droga.

Num período de oito meses, esta investigação conjunta entre os três escritórios regionais da Polícia Estatal de *New Jersey*, sumarizou mais de 8.000 horas de trabalho de vigilância eletrónica, mais de 1.200 horas de escutas telefónicas e mais de 2.300 horas de vigilância física. Cerca de 300 horas foram necessárias para se desenvolveram estratégias a fim de manter as fontes confidenciais. A definição de estratégica de prioridades, o compartilhamento de dados entre agências e a análise e o processamento dos dados recolhidos, permitiu identificar os elementos pertencentes à rede, resultando na prisão de quase 100 indivíduos do gangue dos *Bloods*, enfraquecendo a sua liderança em todo o Estado.

Avaliando pelo número de prisões e pelo desmantelamento de uma organização criminosa, a investigação liderada pela *intelligence* revelou-se um verdadeiro caso de sucesso. Mostrou que é possível o uso de uma avaliação estratégica para melhor definir prioridades também elas estratégicas e que a troca de informação constante entre vários analistas, dentro e fora das suas instituições/organizações, acaba por auxiliar na tomada de decisões.

Anteriormente, a Polícia Estadual não criava prioridades estratégicas para melhor definir áreas de atuação, mas com a implementação do *intelligence-led policing* ficou demonstrado que a definição destas prioridades, facultadas pelo trabalho realizado pelos analistas, nomeadamente na recolha e análise de informação, pode contribuir para uma maior eficácia da atuação policial. Isto vai permitir uma tomada de decisão baseada na informação recolhida, o que acaba por ser a grande diferença com outros modelos de policiamento.

Assim, podemos afirmar, através deste exemplo, que o *intelligence-led policing* poderá ter um papel preventivo no combate ao crime violento e organizado e no combate, às cada vez mais constantes, ameaças globais.

No entanto, identificam-se seguidamente três estudos empíricos, baseados numa abordagem qualitativa, que apontam os desafios que o *intelligence-led policing* enfrenta, nomeadamente quanto aos dados, ao compartilhamento, às ferramentas, às fontes e aos decisores.

A investigação etnográfica de Sanders et, al (2015) pretendia analisar a aplicação do *intelligence-led policing* no contexto canadiano.

Para o efeito, os investigadores realizaram 86 entrevistas em profundidade a analistas, agentes de patrulha e trabalhadores civis de seis departamentos policias. Por motivos de

confidencialidade, os departamentos não foram identificados. As entrevistas foram ainda suplementadas com 36 horas de observação em carros patrulha e com a análise documental. Neste estudo, Sanders et al. (2015) concluíram que a cultura ocupacional e o contexto organizacional da polícia influenciam o sucesso da transição para o novo modelo. Apesar da eficácia deste modelo residir na recolha e troca de informação, os vários departamentos parecem não aceder facilmente a esta partilha. Mesmo entre analistas isto parece acontecer, pois todos querem ser responsáveis por uma grande operação ou detenção. Ou seja, mesmo havendo meios tecnológicos de armazenamento e partilha de dados, devido à norma ocupacional de segredo dentro dos departamentos, essa tecnologia não é usada em todo o seu potencial. Além disso, para Sanders et al. (2015), a inexistência de um relatório comum, dificulta a comunicação de informações entre agências, agravando os problemas de compartilhamento.

O estudo identificou ainda que a falta de recursos tecnológicos impacta negativamente o potencial do modelo, visto que prejudica a qualidade da informação.

Os participantes do estudo salientam também que as organizações são muito dependentes dos analistas para que os dados sejam analisados. No entanto, existe simultaneamente um fraco conhecimento dos líderes sobre o seu papel na construção do conhecimento sobre o crime, nomeadamente como é que estes recolhem a informação, o que é que registam e o que é que fica por registar. Esta ausência de clareza de informação sobre as funções dos analistas de *intelligence*, dificulta o entendimento da sua importância pelos decisores, agravando a sua incompreensão e desconsideração. Assim Sanders et al. (2015), alertam para a necessidade dos decisores valorizarem e implementarem o *intelligence-led policing*, salientando que este carece de um bom suporte organizacional.

Já Burcher e Whelan (2018) concretizaram um estudo que tencionava explorar a aplicação do modelo na Austrália. Os autores realizaram entrevistas em profundidade a 27 analistas de *intelligence* das duas maiores agências policiais estaduais australianas: 17 elementos da *Victoria Police* e 10 elementos da *New South Wales Police Force*.

O estudo de Burcher e Whelan (2018), à semelhança da investigação de Sanders et al. (2015), concluiu que a troca de informações inter e intragências é uma prática pouco frequente nas agências australianas.

Para Burcher e Whelan (2018), a qualidade da informação também é influenciada pela existência dados incoerentes e/ou inválidos ou pela ausência de informações relevantes. Além disso, o estudo aponta o crescente uso das redes sociais enquanto fontes de informação

como uma das principais causas para a sobrecarga dos sistemas de *intelligence* com dados inúteis.

Os entrevistados apresentaram ainda críticas relativas às ferramentas disponibilizadas pelas agências. Mais concretamente, de acordo com os relatos recolhidos, os equipamentos tecnológicos disponibilizados pelas organizações possuem uma capacidade fraca, o que condiciona gravemente a análise das informações e impede os analistas de usufruir de *softwares* mais sofisticados e aplicar técnicas de análise mais avançadas.

Burcher e Whelan (2018) destacam também a fraca relação de compreensão entre os analistas e os chefes de polícia. De acordo com os relatos dos analistas, os líderes da polícia, principalmente os mais velhos, não consideram os saberes da *intelligence* na tomada de decisões, pois não conseguem identificar as suas vantagens. Isto acentua o clima de desconfiança entre analistas e líderes.

Por sua vez, Cope (2004) concentrou-se no estudo do *intelligence-led policing* e do processo de compartilhamento de informações no Reino Unido, por meio de unidades de *intelligence:* uma numa força municipal e outra numa força urbana.

Neste estudo, o principal método utilizado foi a observação participante que ocorreu durante um período de dois meses nas unidades referidas. Além disso, foram realizadas entrevistas semiestruturadas a 16 analistas, 9 oficiais de *intelligence filed*, 7 informantes e 6 líderes das unidades de *intelligence* e superintendentes responsáveis por conduzir o processo de atribuição de tarefas. Foram ainda realizadas entrevistas informais aos funcionários responsáveis pelos sistemas de *intelligence* baseados nos computadores e aos polícias que responderam às tarefas.

No estudo de Cope (2004), os profissionais de *intelligence* relataram que nem sempre têm acesso às informações completas, devido à fraca ou quase inexistente prática de compartilhamento de informações. A pobre de troca de dados e a exclusão de conteúdos sensíveis da análise são dois dos principais fatores que contribuem para a má qualidade da informação.

Cope (2004) percebeu também que os desafios relacionados com os analistas surgem ainda na fase de recrutamento, dado que as agências se centram nos licenciados com a esperança de que os diplomas forneçam todas as habilidades que um analista precisa, por exemplo, saber pensar analiticamente e processar várias fontes de informação. Os analistas entrevistados por Cope (2004) consideram que a experiência em trabalho de *intelligence* é um dos critérios mais importantes para ser um bom analista, contestando que as organizações apenas se importem com os diplomas.

À semelhança das investigações anteriores, os entrevistados do estudo de Cope (2004) relataram que, frequentemente, o produto *intelligence* é ignorado e não influencia as decisões dos líderes relativamente à intervenção no ambiente criminal. A alienação ao produto i*ntelligence* torna-se ainda mais evidente quando é revelado pelos participantes que raramente os analistas recebem *feedback* dos supostos consumidores de *intelligence.*

Assim, as investigações permitiram concluir que a fraca qualidade da informação e a falta de compreensão das habilidades dos analistas não permitem aos líderes entender a importância do seu papel. De acordo com os relatos dos profissionais, muitas vezes o produto *intelligence* foi utilizado após a intervenção no ambiente criminal, servindo apenas para justificar uma operação já planeada (Cope, 2004).

Deste modo, embora o *intelligence-led policing* apresente um conjunto de princípios e orientações basilares, frequentemente estas orientações não são aplicadas na prática, devido às necessidades existentes, sendo necessário que investigações futuras procurem explorá-las.

Com o advento do *big data*, a recolha e análise de grandes volumes de dados de diversas fontes permitiram uma compreensão mais profunda e em tempo real das atividades criminais. Essa integração melhorou a capacidade de prever e prevenir crimes, tornando as forças de segurança mais eficientes e proativas.

Para Chi (2019), o valor do uso do *big data* no policiamento apresenta-se em três dimensões, nomeadamente a integração e compartilhamento de dados, uma vez que o *big data* permite a consolidação dos dados, colmatando dados incompletos ou errados e contribuindo para um compartilhamento mais eficaz. Assim, cria-se um sistema integrado, em que os dados podem ser compartilhados e utilizados de forma mais eficiente para combater a criminalidade; O apoio técnico na compreensão de informações sociais, isto porque a polícia pode, através do *big data*, realizar análises avançadas e detetar padrões de criminalidade, tendências sociais e ofensores prolíficos. Essa interpretação do meio permite que as medidas táticas e estratégicas implementadas no meio sejam mais eficazes para combater a criminalidade, centrando-se nas causas dos problemas; E o auxílio na tomada de decisões, já que os decisores devem considerar os dados analisados na tomada de decisões para que as medidas táticas e estratégicas implementadas sejam eficazes. O produto *intelligence* permite que os líderes da polícia tomem decisões mais informadas e baseadas em evidências, quer relacionadas ao direcionamento de recursos ou ao planeamento estratégico e tático.

O uso do *big data* na repressão e prevenção criminal transformou o policiamento, implementando uma abordagem da segurança pública mais integrada, informada e eficaz

para o combate aos novos desafios. Este permite que os corpos da polícia se tornem mais proativos, eficientes e eficazes na proteção das comunidades.

Neiva, Granja e Machado (2022), apresentam o uso de *big data* nas seguintes atividades de policiamento: Informar sobre tendências futura, visto que os polícias utilizam os dados processados para prevenir determinados fenómenos, implementando medidas táticas e estratégicas eficazes que incidem nas causas dos problemas. Destaca-se a proatividade da polícia moderna; Fornecer dados variados, uma vez que o *Big Data* resulta da recolha de uma grande quantidade de dados variados, ou seja, os dados não somente podem ter sido recolhidos por diversas fontes, por exemplo, câmaras de segurança, redes sociais, entre outras, como podem apresentar vários formatos, texto, vídeo, etc. Esses dados devem ser analisados, através de *software*s avançados, em tempo real para a identificação de atividades criminosas em curso e para a detenção em flagrante delito; e Expandir o alcance das bases de dados de ADN, já que o *big data* pode permitir a deteção e apreensão de criminosos em casos passados, uma vez que o cruzamento de grandes quantidades de dados genéticos pode permitir correspondências entre amostras de ADN. Deste modo, o *big data* pode assumir-se como uma ferramenta importante na resolução de casos antigos e na identificação de criminosos que de outra forma poderiam permanecer impunes.

O *big data* assume um valor transformador na maximização da eficácia da polícia, visto que o fornecimento de *insights preditivos*, permitem a alocação de recursos técnicos e humanos consoante as necessidades, incidindo-se sobre as causas do problema e potenciando a segurança e a justiça das comunidades.

Não obstante, é essencial reconhecer que o uso desta ferramenta avançada no policiamento apresenta desafios e preocupações (Wout et al., 2021). Neste sentido, questões relacionadas à privacidade, enviesamentos do algorítmico e transparência devem ser abordadas de forma cuidadosa e responsável para garantir que os direitos fundamentais dos cidadãos são protegidos.

Assim, as análises baseadas em *big data* são uma prática que se tem proliferado e desenvolvido ao longo dos tempos e que permitem que a segurança pública assente nos princípios da prevenção criminal baseada na gestão de risco.

Um exemplo do uso do *big data* no combate às ameaças globais é o *Projeto Total Information Awareness*. Este projeto, inicialmente direcionado para o terrorismo, tem como objetivo desenvolver um sistema de vigilância massiva capaz de identificar e prevenir atividades terroristas, através da recolha e análise de vastas quantidades de dados (Costa,

2004). Assim, a recolha e análise de grandes quantidades de dados permite ao governo, vigiar potenciais terroristas, prevenindo o cometimento de ofensas.

No entanto, os estudos sobre as perspetivas dos polícias sobre o uso do *big data* no policiamento são escassos. Dos poucos estudos apresentados na literatura científica, apontam-se dois trabalhos sobre esta matéria.

O estudo de Brayne (2017) tem como objetivo explorar a relação entre o crescimento da vigilância e a ascenção do *big data*. Para o efeito, a autora, ao longo de dois anos e meio, conduziu um estudo qualitativo em que realizou observações e entrevistas a 75 polícias do Departamento da Polícia de *Los Angeles* e ainda realizou entrevistas de acompanhamento com uma subamostra de 31 polícias para acompanhar como é que determinadas tecnologias foram disseminadas e como é que as informações são compartilhadas.

Brayne (2017), concluiu que o uso *big data* proporcionou uma mudança de paradigma, uma vez que alterou os princípios de atuação da polícia, destacando-se os seguintes aspetos: a Polícia de *Los Angeles* passou a realizar a gestão do nível de risco dos suspeitos, a priorizar o policiamento preditivo, a usar o *big data* nas usas análises, a realizar análises em rede e construiu um sistema integrado, em que o compartilhamento de dados é essencial.

Já o estudo de Chan & Moses (2017), explora as perceções dos polícias sobre o uso do *big data* na polícia da Austrália. Para o efeito, realizaram 31 entrevistas semiestruturadas a 38 partes interessadas, nomeadamente autoridades da polícia e da *intelligence*, agência de supervisão de oficiais, legisladores, informáticos e oficiais da sociedade civil. Destas, somente 24 entrevistas foram gravadas com o consentimento dos participantes, sendo que para o resto foram tomadas notas, a fim de recriar o mais fielmente possível as palavras usadas pelos participantes.

O estudo de Chan & Moses (2017) aponta a falta de tempo e de recursos como fatores que criam resistência à mudança de paradigma e conclui que a comunidade deve assumir um papel mais ativo na compreensão do *big data* e encorajar o seu uso. Contudo, os participantes parecem reconhecer o valor do *big data* como uma ferramenta avançada que permite uma abordagem mais proativa da segurança, baseada em inferências sobre tendências e padrões.

Deste modo, Chan e Moses (2017) apontam que, embora as promessas de eficácia e eficiência do *big data* no policiamento, pouco se sabe sobre os desafios que o seu uso apresenta na prática, sendo necessários mais estudos que procurem compreender as perspetivas e expectativas dos polícias sobre esta matéria.

À semelhança do que acontece no panorama internacional, os estudos portugueses sobre esta matéria também são escassos, destacando-se o estudo de Pereira (2019) que tem como

objetivo compreender a implementação e o desenvolvimento do sistema de informação central na Polícia de Segurança Pública. Para isso, Pereira (2019) realizou uma análise de conteúdo do Plano Estratégico de Sistemas de Informação (PESI), o Estudo SEI+ - Estudo de Utilização e Evolução do SEI.

O autor (Pereira, 2019) concluiu que apenas a avaliação das tecnologias e a objetividade da análise não constam nos documentos analisados, o que evidencia a necessidade de que estes segmentos precisam de ser desenvolvidos pela Polícia de Segurança Pública, isto porque a avaliação das tecnologias evita a cristalização dos sistemas, obedecendo há necessidade do Sistema Estratégico de Informação em acompanhar os desenvolvimentos tecnológicos, e a objetividade da análise é fundamental para que a análise seja isenta e livre de convicções pessoais e ideologias que a possam enviesar (Pereira, 2019). Assim, é essencial que estes dois aspetos constem nos documentos estratégicos de implementação e desenvolvimento do Sistema Estratégico de Informação.

Deste modo, embora o *big data* permita alterar o paradigma de policiamento e os princípios para o combate à criminalidade, o seu uso pelos corpos da polícia parece apresentar algumas resistências que as investigações futuras devem explorar.

3. Desafios éticos, legais e sociais

Projetos como o *Total Information Awareness* que utilizam o *big data* para a vigilância de potenciais ofensores (Costa, 2004), levantam questões relacionadas com os direitos fundamentais dos cidadãos. Não obstante, o reconhecimento do valor do *big data* no policiamento pela comunidade científica, os estudos apontam riscos associados ao seu uso. Além disso, parecem existir aspetos técnicos e legais que condicionam a sua utilização pela polícia. Por exemplo, no seu relatório, Babuta (2017) consciencializa para a ausência de regulamentação sobre o uso do *big data* pelas forças de segurança do Reino Unido (Babuta, 2017).

À semelhança do que acontece no Reino Unido, em Portugal, também não existe um quadro normativo que preveja os termos desta aplicação. No entanto, o artigo 272º, nº3 da Constituição da República Portuguesa (CRP) e o artigo 2.º da Lei de Segurança Interna ditam que em Portugal não é permitido à polícia, ainda que por razões securitárias, exerça uma vigilância constante, permanente e ininterrupta da população, salvaguardando-se o direito à liberdade, à privacidade e à presunção de inocência, consagrados pela CRP.

Este assunto tem suscitado trabalhos reflexivos na literatura, a qual medeia um debate científico que se define numa medição de forças entre as vantagens do *big data* e os males

da sua aplicação. Ora, se por um lado o *big data* melhora a capacidade preditiva e preventiva da polícia, tornando-a mais eficaz no combate ao crime, por outro lado a sua adoção nas atividades da polícia pode levantar problemas de origem diversa, seja éticos, sociais e/ou legais, desencorajando o seu uso (Herschel & Miori, 2017).

Um dos desafios debatidos concentra-se desde logo na fase da recolha dos dados, isto porque os estudos alertam que os dados recolhidos e armazenados nas bases de dados podem estar enviesados. Por razões históricas, sociais e culturais o policiamento não assume uma distribuição igual pela sociedade (Brayne, 2017). Por exemplo, um indivíduo negro com baixo estatuto socioeconómico e que viva num bairro social merecerá mais atenção da polícia (Brayne, 2017) do que um indivíduo branco com elevado estatuto socioeconómico e que viva numa zona nobre. Ora, se alguns grupos sociais, por motivos raciais e socioeconómicos, são mais vigiados do que outros, a probabilidade de serem detetados comportamentos criminosos é também maior nestes do que noutros.

No entanto, ainda que sejam detetados mais crimes, não significa necessariamente que estes grupos sociais cometam mais crimes. Deste modo, uma vez que os sistemas tecnológicos se baseiam em algoritmos e que os dados recolhidos estão enviesados, o *software* interpreta que determinados sujeitos ou comunidades, em razão de aspetos raciais e socioeconómicos, devem ser considerados suspeitos, ainda que isso não corresponda à realidade. Se a polícia utilizar estes dados sem refletir sobre os mesmos, corremos o grave risco de o policiamento ser orientado por previsões distorcidas e que fogem à realidade criminal (Boyd & Crawford, 2012).

Além disso, estas previsões distorcidas podem levar à implementação de políticas criminais desiguais e discriminatórias que se centram em "comunidades suspeitas" (Machado et al., 2020). Neste sentido, se um indivíduo pertencer a uma "comunidade suspeita" passa a ser entendido como uma potencial ameaça, sendo exercido um maior controlo e vigilância sobre o mesmo (Skinner, 2013). Por outras palavras, um indivíduo pode ser visto como suspeito sem que tenha adotado qualquer comportamento desviante, sendo suficiente que reúna certos aspetos raciais e socioeconómicos (Boyd & Crawford, 2012). Assim que é rotulado como suspeito, o sujeito passa a ser alvo de uma vigia permanente e ininterrupta, violando-se grosseiramente o seu direito à liberdade, privacidade e presunção de inocência (Neiva, Granja e Machado, 2022).

Contudo, quando consideramos que todos aqueles que pertençam à rede de contactos do dito suspeito também passam a ser alvo de controlo (Brayne, 2017), entendemos que os sistemas tecnológicos podem constituir verdadeiras armas de vigilância em massa.

Outro desafio abordado na literatura prende-se com a questão da voluntariedade de cedência dos dados, pois mesmo nos casos em que os dados são recolhidos por via de fontes abertas ao público como as redes sociais, a voluntariedade da sua cedência pode ser questionada, visto que quem os divulga pode não aceitar/concordar com todos os fins que esses dados podem servir (Bauman et al., 2014). Ou seja, quando não há uma total consciência sobre os diversos fins que os dados podem servir, a voluntariedade da sua cedência fica fragilizada (Lyon, 2014).

Mais se acrescenta que o Tribunal Europeu dos Direitos Humanos declarou que este tipo de fonte de dados viola o direito à privacidade e que, por isso, não deve ser utilizada pela polícia para efeitos de investigação, salvo casos em que as entidades apresentem uma justificação rigorosa para tal (Vermeulen & Lievens, 2017).

Um outro desafio relaciona-se com aqueles crimes que, por não serem reportados ou por ocorrerem no âmbito de atividades legítimas, ficam fora das malhas da vigilância. Por serem menos visíveis, estes crimes não integram o algoritmo dos sistemas tenológicos, não aparecem nas prioridades de investigação da polícia e permanecem sem resolução.

Um último desafio prende-se com o facto de os países possuírem quadros legislativos e princípios de governação, infraestruturas tecnológicas e imperativos e princípios organizacionais diferentes, o que pode ter um impacto nas expectativas sobre o *big data* dos profissionais (Neiva, Granja e Machado, 2022). Neste sentido, é necessária uma análise da forma como os diferentes países estão a conceber, mobilizar e integrar o *big data* nas práticas da polícia (Neiva, Granja e Machado, 2022), isto porque compreender a diversidade de expectativas dos polícias sobre o *big data* antes da sua implementação pode contribuir para uma governança mais eficaz, antecipando-se a resolução de problemas e dificuldades e colmatando necessidades.

Posto isto, embora a aplicação do *big data* no policiamento possa contribuir com múltiplos benefícios, o debate presente na literatura elucida-nos para o facto do seu uso poder também exacerbar desigualdades socias, incitar à discriminação e atentar as garantias e liberdades dos cidadãos.

Assim, se por um lado o desenvolvimento tecnológico contribui com achados inovadores e muito relevantes para as mais diversas áreas, munindo-as de técnicas e *softwares* sofisticados que melhoram as suas atividades, por outro lado também levanta também rigorosos, árduos e complexos desafios éticos, socias e legais que podem condicionar a sua própria aplicação, dado que o uso de uma tecnologia, ainda que por razões securitárias, não pode violar os direitos dos indivíduos, exigindo-se sempre reflexão nesse sentido (Wout et al., 2021).

Deste modo, ainda que o *big data* possa ter potencial para aperfeiçoar a capacidade preditiva e preventiva da polícia, este também corre o risco de acentuar fossos de desigualdade social e o desrespeito pelos direitos fundamentais dos cidadãos, minando a confiança dos cidadãos na polícia.

Além disso, face ao debate levado a cabo na literatura que enumera não só os potencias uso do *big data*, mas ainda as vantagens e desvantagens do seu uso no policiamento, será importante compreender as perspetivas dos polícias sobre tais questões, visto que as suas perceções e opiniões podem incentivar ou desencorajar a aplicação desta tecnologia nas atividades da polícia (Neiva, 2019).

PARTE II – ESTUDO EMPÍRICO (METODOLOGIA)

1. Objetivos e questões de investigação

De acordo com Neiva (2019), as perspetivas e as expectativas dos polícias sobre o uso do *big data* no policiamento podem potenciar ou desencorajar a sua utilização. No entanto, as perceções dos polícias podem ser influenciadas pelos quadros legislativos e princípios de governação, infraestruturas tecnológicas e imperativos e princípios organizacionais que variam de país para país (Neiva, Granja e Machado, 2022).

Deste modo, o presente estudo tem como objetivo compreender as perspetivas e expectativas dos polícias sobre o uso do *big data* na prevenção e investigação criminal no contexto português, baseando-se nas seguintes questões de investigação: compreender como é que os polícias entendem o conceito do *big data*, nomeadamente como é que o definem e quais os benefícios do seu uso; perceber o papel dos analistas, mais especificamente que tipo de formação e habilidades possuem; entender as ferramentas usadas, nomeadamente identificar que tipo de técnicas são usadas e qual a sua qualidade, e aceder às fontes de dados usadas, concretamente identificar quais as fontes de dados usadas, qual a sua qualidade, como se processa o compartilhamento dos dados e quais os desafios éticos, legais e sociais encontrados pelos polícias.

2. Operacionalização: instrumentos

Para procurar responder às questões de investigação, optou-se por utilizar uma metodologia qualitativa, uma vez que é o método mais adequado para se aceder às perspetivas e expectativas dos polícias sobre o uso do *big data* na prevenção e investigação criminal, isto porque este tipo de abordagem qualitativa busca entender os significados que os indivíduos atribuem aos fenómenos.

Além disso, optou-se pela realização de entrevistas semiestruturadas aos polícias, uma vez que este seria o método mais adequado para servir os objetivos do presente estudo, nomeadamente a procura de descrições ricas de informação e das perspetivas dos entrevistados sobre o objeto do estudo (Petinseva et al., 2020).

Assim, dado que as entrevistas semiestruturadas assentam num guião de entrevista, selecionei um conjunto de questões que abordavam e exploravam as dimensões de interesse para o estudo e que foram colocadas durante as entrevistas aos participantes.

Não obstante, ainda que exista um guião, as entrevistas semiestruturadas não possuem uma estruturada fechada, por isso, durante as entrevistas, as dimensões do guião foram abordadas de forma flexível, não existindo uma sequência linear rigorosa.

Além disso, devido à flexibilidade das entrevistas semiestruturadas para a consideração de outras dimensões que não estavam previstas no guião, mas que foram levantadas pelos entrevistados durante as entrevistas, explorei algumas dimensões que não se encontravam previstas no guião construído (Kvale, 1996). Neste sentido, procurei, como sugerido por Petinseva et al. (2020), que os polícias decidissem livremente o que era valioso como resposta.

Note-se ainda que as novas dimensões abordadas pelos polícias, quando relevantes para o objetivo do estudo, foram consideradas nas entrevistas posteriores, contribuindo para o aperfeiçoamento do guião (Petintseva et al., 2020). Por exemplo, uma subdimensão incluída no guião e que não se encontrava inicialmente prevista, designa-se "necessidades de formação", isto porque quando questionados sobre o tipo de formação que os analistas possuíam, os entrevistados apontavam que estes profissionais necessitariam que a instituição da Polícia de Segurança Pública fornecesse formação contínua, em determinadas áreas específicas.

Importa ainda mencionar que, apesar do conhecimento que obti sobre o tema durante a realização do enquadramento teórico, durante a entrevista não partilhei nenhum dos meus conhecimentos com o entrevistado (Petinseva et al., 2020), evitando o enviesamento dos dados.

Assim, quanto ao guião de entrevista usado no presente estudo, este foi construído com vista a responder aos objetivos da presente dissertação e baseado nos achados da literatura científica. Deste modo, o guião de entrevista utilizado engloba as seguintes dimensões: o conhecimento que os polícias possuem sobre o *big data*, os atores realizam as análises baseadas no *big data*, as ferramentas que são utilizadas nas análises e as fontes de dados que são usadas para recolher os dados. Cada dimensão, divide-se em subdimensões que procuram explorar o seguinte: na primeira dimensão procura-se perceber como é que os polícias entendem o *big data*, nomeadamente como é que o definem e quais são os benefícios que encontram no seu uso pela polícia. Esta dimensão e respetivas subdimensões procuram perceber se as perspetivas dos polícias sobre o *big data* são positivas, na medida em que estas opiniões podem encorajar ou desencorajar o seu uso pelos profissionais (Neiva, 2019). A segunda dimensão trata dos profissionais que analisam o *big data*, os analistas, procurando-se, mais especificamente, perceber que tipo de formação e habilidades possuem estes profissionais, já que, segundo Cope (2004), a formação e experiência do analista é muito importante para que este saiba interpretar a informação extraída dos dados e consiga apresentá-la ao comandante, de modo a orientar as suas decisões.

A terceira dimensão procura explorar as ferramentas usadas pelos analistas nas suas análises, nomeadamente perceber que tipo de técnicas são usadas e qual a qualidade desses recursos, isto porque os estudos de Burcher & Whelan (2018) e Sanders et al. (2015) apontam a falta tecnologias avançadas como um entrave ao uso do *big data* no policiamento.

A quarta dimensão pretende compreender quais as fontes de dados usadas pelos analistas para recolher os dados, mais concretamente que tipo de fontes, qual a sua qualidade, como ocorre o compartilhamento de dados e quais os desafios éticos, legais e sociais que os analistas encontram. Inicialmente, é essencial perceber a origem dos dados, visto que a sua origem pode levantar problemas quanto à sua validade e certos desafios legais sociais e éticos (Wout et al.,2021). Depois, é também importante questionar os profissionais sobre o compartilhamento, visto que, de acordo com Chi (2019), esta é uma prática importante para a promoção da sinergia dos vários departamentos da polícia, transformando um sistema de governança social fragmentado num sistema integrado. Além disso, Cope (2004) refere que a ausência de compartilhamento contribui para a má qualidade da informação.

Por fim, entendi ser ainda necessário criar uma dimensão, designada "direções futuras", que tem como objetivo dar espaço ao participante para apresentar outros assuntos sobre o objeto de estudo que não foram questionados ou para clarificar alguma informação dada.

3. Amostra e procedimentos

Para a realização do estudo foi pedido o aparecer à Comissão de Ética da FDUP, de modo a garantir que o estudo respeita os direitos e o bem-estar dos participantes e que se encontra em conformidade com os padrões éticos estabelecidos pela Universidade do Porto.

Após a autorização da Comissão de Ética para a realização do estudo, contactei via e-mail o Comando Metropolitano do Porto da Polícia de Segurança Pública, de modo a pedir autorização à respetiva instituição para a realização do estudo e para a nomeação de 6 profissionais da Polícia de Segurança Pública com cargos distintos, nomeadamente um comandante, um analista e um agente, e que possuíssem conhecimento e experiência na área do *big data* na prevenção e na investigação criminal.

Mencionei ainda que seria essencial que os polícias nomeados possuíssem conhecimento e experiência relevante com o *big data*, isto porque, de acordo com Machado (2004), a amostra deve ser constituída por sujeitos capazes de fornecer informação sobre o fenómeno em estudo. Os participantes devem possuir um conjunto de características e critérios que permitam o desenvolvimento da investigação (Machado, 2004).

Além disso, anexo ao e-mail do pedido de autorização direcionado à instituição Polícia de Segurança Pública, procedi ao envio do consentimento informado, em que apresentava o projeto e a instituição que acolhe o projeto, a Faculdade de Direito da Universidade do Porto, onde referia a realização de entrevistas para explorar o objeto do estudo, mencionava a duração esperada para cada entrevista e apresentava uma breve descrição dos procedimentos de recolha de dados e proteção dos mesmos. Além disso, explicitava, de forma clara e evidente, a voluntariedade da participação dos profissionais, a sua possibilidade de desistência e assegurava a confidencialidade dos dados e o anonimato.

É ainda mencionado que, no caso de dúvidas, existia a possibilidade do agendamento de uma reunião prévia às entrevistas para o esclarecimento de eventuais dúvidas.

As entrevistas foram realizadas entre abril e maio de 2024, ajustando-se à disponibilidade dos polícias.

Assim, a amostra do presente estudo foi constituída por 6 polícias da Polícia de Segurança Pública, nomeadamente 3 profissionais da Divisão de Investigação Criminal e 3 profissionais do Núcleo de Informações Policiais do Comando Metropolitano do Porto.

A nomeação de profissionais de diferentes divisões da Polícia de Segurança Pública, uns mais focados na investigação criminal e outros na área da prevenção, respetivamente, e com cargos distintos teve como objetivo o enriquecimento do estudo com diferentes perspetivas e experiências do uso do *big data* no policiamento. Deste modo, a amostra era intencional, dado que os participantes foram selecionados com base em critérios previamente definidos (Patton, 1991).

As entrevistas aos polícias foram realizadas individualmente, numa sala de cada divisão da polícia, sendo que a mesma foi escolhida pelos entrevistados. Esta sala era um local que obedecia às condições mínimas para que a entrevista não fosse prejudicada, visto que era um local silencioso, seguro e onde o entrevistado se poderia sentir confortável.

Note-se ainda que a duração média das entrevistas foi de aproximadamente de 30 minutos e que todas foram realizadas em português, não sendo necessário qualquer tradutor.

No início de cada entrevista foram repetidos alguns elementos do consentimento informado para assegurar a voluntariedade da participação dos profissionais, relembrar questões éticas como o anonimato e confidencialidade e solicitar a autorização do participante para a gravação da entrevista por áudio.

A gravação visava facilitar a recolha dos dados que foram posteriormente transcritos. As gravações foram guardadas num lugar seguro, ao qual só eu e a minha orientadora tínhamos acesso e, após a transcrição dos dados, foram apagadas.

Todas as entrevistas foram transcritas por mim, sem recurso a qualquer *software*.

4. Análise dos dados

A análise dos dados baseou-se no método de análise temática, uma vez que esta permite identificar, analisar e reportar os padrões nas informações fornecidas pelos polícias (Braun & Clarke, 2006). Ou seja, este método analítico qualitativo permitiu-me organizar e descrever detalhadamente as informações ricas dadas pelos entrevistados.

Assim, a análise das entrevistas assentou em 6 etapas, não sequenciais e que se articulavam entre si (Patton, 2005), que tinha como objetivo identificar os temas que agregavam o material qualitativo previamente codificado e que permitiram, posteriormente, o desenvolvimento de um argumento teórico. Deste modo, os dados recolhidos foram organizados categoricamente, a fim de produzir conhecimento sobre o objeto de estudo.

Note-se que durante a análise temática das entrevistas, devido à articulação entre as diferentes fases do método, existiram avanços e recuos constantes entre as diversas fases do método, tratando-se, portanto, de um processo flexível (Braun & Clarke, 2006).

Como referido, a análise temática incluiu 6 etapas distintas, nomeadamente a familiarização com o material qualitativo, a codificação dos dados, a organização dos códigos, a refinação dos temas, revisão dos temas e análise dos temas e redação dos resultados (Braun e Clarke, 2006).

Deste modo, a fase 1 centrou-se na familiarização com o material qualitativo, sendo a primeira tarefa realizada a transcrição das entrevistas aos polícias. Esta tarefa foi morosa, mas não é desperdício de tempo, visto que é essencial para a familiarização com os dados, permitindo uma interpretação e análise prévia dos mesmos (Braun & Clarke, 2006). Note-se que as transcrições foram realizadas por mim, sem recurso a qualquer *software*.

O foco nos dados durante a sua transcrição, permitiu-me estar desperta para os dados mais subtis (Tuckett, 2005).

Além disso, durante a leitura e análise prévia dos dados, retirei notas sobre cada entrevista realizada, identificando ideias importantes para a fase de codificação (Braun & Clarke, 2006). Concluída esta etapa, avancei para o passo seguinte.

Na fase 2, codificaram-se os dados, ou seja, organizaram-se os dados em grupos de significado (Tuckett, 2005).

Dado que para Boyatzis (1998), um código é "o segmento ou elemento mais básico dos dados brutos que pode ser avaliado de maneira significativa com relação ao fenómeno sob estudo",

os códigos definidos foram provenientes da familiarização com os dados, da literatura científica e das categorias gerais do guião de entrevista (Braun & Clarke, 2006).

Optou-se por esta abordagem mista, uma vez que esta permitiu, simultaneamente, valorizar a teoria presente na literatura, mas também os novos dados que surgiram durante as entrevistas. Além disso, os códigos foram construídos por mim, não usufruindo de qualquer *software* para o efeito.

Após a colocação de cada frase e excerto nos respetivos códigos. Avancei para a fase seguinte.

A fase 3, dedicou-se à organização dos códigos em temas mais amplos (Braun & Clarke, 2006), debatendo-se a relação entre os códigos, os temas mais largos e os subtemas. Note-se que, de acordo com Braun e Clarke (2006), os códigos excluídos foram integrados numa outra secção criada para esse propósito, designada "outros temas".

A fase 4, centrou-se na refinação dos temas, sendo necessária a releitura das entrevistas. Os temas atenderam aos critérios de homogeneidade interna e heterogeneidade externa de Patton (2015), de modo a formarem um padrão coerente. Neste sentido, apesar de apresentarem algo em comum, os temas também assumiam distinções claras entre eles.

Assim, a fase 4 baseou-se em dois níveis: na definição de temas coerentes face aos dados e na codificação dos dados perdidos nas fases anteriores, de modo a integrá-los nos temas (Braun & Clarke, 2006). No entanto, este processo de revisão e refinamento dos temas não pode prosseguir *ad infinitum* (Souza, 2019), sendo que quando considerei que nada mais havia a alterar, terminei esta etapa e avancei para a seguinte.

A fase 5 tratou-se de um processo de revisão e refinamento dos temas (Braun & Clarke, 2006), sendo que esta só terminou quando os temas definidos cumpriam os critérios de homogeneidade interna e heterogeneidade externa de Patton (2015), indiciados anteriormente. Os temas finais apresentaram-se como concisos e diretos, evitando-se a sobreposição de temas.

A última etapa, foi a fase 6 que se ocupou da análise dos dados e da redação dos resultados, considerando-se que esta deveria de ser objetiva, coerente e lógica, mas ultrapassar a superfície dos dados, acrescentando mais do que a sua mera descrição (Braun e Clarke, 2006).

PARTE III – ESTUDO EMPÍRICO (RESULTADOS)

1. Resultados

Conhecimento sobre o big data

Inicialmente, foi solicitado a todos os participantes para definirem o conceito *big data*.

O objetivo seria compreender de que forma os polícias percebiam o objeto de estudo, dado que a forma como o definem pode influenciar as respostas dadas às questões seguintes.

As respostas apresentadas quanto à definição do *big data* foram semelhantes entre os participantes, tendo definindo o conceito como um grande conjunto de dados que são analisados e processados, através de tecnologias, para produzir informação que oriente. Todas as definições dadas pelos entrevistados apontam o volume como um aspeto basilar do conceito, isto porque, todos os polícias consideram que *big data* corresponde a uma grande quantidade de dados.

No entanto, mais de metade dos polícias identificam outros dois aspetos essenciais que definem o *big data*, nomeadamente a variedade dos dados e a velocidade do processamento dos dados. Assim, a maioria dos participantes define *big data* como um grande conjunto de dados variados que são analisados e processados rapidamente, através de tecnologias, e que produzem informação que orienta.

Outra questão colocada aos polícias centrou-se na aplicabilidade do *big data* ao policiamento, procurando-se perceber como é que os dados podem ser utilizados na prevenção e na investigação criminal.

Deste modo, os entrevistados indicaram que a análise e o processamento do *big data* permite à polícia detetar padrões nos dados, identificando quais os crimes cometidos, quem comete esses crimes, em que local, a que horas, quando os comete e porque é que os comete, auxiliando na implementação de estratégias operacionais e preventivas e no direcionamento de recursos técnicos e humanos. Assim, para os polícias o *big data* permite estabelecer um modelo de policiamento em que a polícia consegue prevenir a criminalidade, através da realização de projeções sobre o crime que se baseiam na interpretação dos dados recolhidos.

As respostas dadas pelos entrevistados apontam o contributo positivo do *big data* para o policiamento, nomeadamente para na área da prevenção do crime, uma vez, de acordo com os polícias, a análise e o processamento dos dados recolhidos permitem o conhecimento dos indivíduos e das áreas geográficas, em termos criminógenos, e podem orientar as estratégias para o combate à criminalidade, podendo proporcionar um policiamento mais profícuo, quer termos de predição do crime ou de direcionamento de recursos humanos e técnicos.

Atores

Foi pedido aos polícias que identificassem o tipo de formação que os analistas possuem, a fim de compreender como é o percurso formativo destes profissionais e que tipo de habilidades e capacidades profissionais possuem, no âmbito do cargo que desempenham. Os entrevistados indicaram que todos os polícias aprenderam a trabalhar com o Sistema Estratégico de Informações, mas que somente os analistas possuem formação em tecnologias de informação para conseguirem trabalhar com *softwares* e cursos em análises de informações policiais ou criminais, dependendo do foco da sua atividade profissional, de modo a conseguirem interpretar os dados e apresentá-los ao comandante para que este tome melhores decisões.

Além disso, as respostas dadas pelos polícias indicam que os analistas devem permanecer em constante atualização académica para acompanhar a evolução da criminalidade e dos recursos tecnológicos. Assim, segundo os polícias, o percurso formativo de cada analista vai-se moldando conforme as suas exigências profissionais e necessidades.

Foi ainda perguntado aos entrevistados se a instituição Polícia Segurança Pública fornecia formação aos analistas, de modo aos profissionais acompanharem a evolução da criminalidade e dos recursos tecnológicos, e que tipo de necessidades formativas eram sentidas pelos analistas.

Os polícias indicaram que a instituição Polícia de Segurança Pública fornece formação aos seus profissionais, mas que não é suficiente, face às necessidades práticas. Ou seja, os entrevistados apontam que, apesar da instituição fornecer aos analistas mais formação do que há 10 anos, além de ser insuficiente para responder às necessidades dos profissionais, também não é disponibilizada a todos os analistas. Os polícias referem que a insuficiente formação dada pela instituição está relacionada com a ausência de investimento do governo na polícia, que se centra noutras prioridades.

Para os participantes as principais necessidades formativas sentidas relacionam-se com o cibercrime, os direitos humanos e o primeiro contacto com a informação. Os polícias indicam que o mundo cibernético está em constante evolução, sendo necessária uma aprendizagem contínua para conseguirem responder às necessidades práticas. No entanto, devido à insuficiente formação que instituição fornece aos analistas sobre a matéria, os profissionais acabam por tirar estes cursos nas suas horas de descanso e a título pessoal.

Os polícias indicam ainda a necessidade da instituição Polícia de Segurança Pública fornecer formação aos analistas no âmbito dos direitos fundamentais para que estejam sensibilizados para os riscos do uso indevido do *big data*, no que respeita aos direitos, liberdades e garantias

dos cidadãos. Os participantes consideram que este tipo de formação é importante para consciencializar os analistas que as necessidades de prevenção e investigação criminal não podem limitar os direitos fundamentais dos cidadãos, pois a sua proteção é importante para a Polícia de Segurança Pública e para o Estado.

Os polícias apontam ainda a necessidade de formações que sensibilizem os profissionais para a necessidade de validar a informação antes de inseri-la nas plataformas de dados da polícia, através do cruzamento de várias fontes de dados.

Ferramentas

Foi solicitado aos polícias que indicassem o tipo de técnicas que são usadas na recolha e análise dos dados recolhidos, para compreender que tipo de recursos técnicos são usados pelos analistas.

Os polícias apontaram que a análise ainda é muito manual, ou seja, ainda se recorre aos métodos tradicionais para recolher e analisar o *big data*. Segundo os participantes, a inserção dos dados nas plataformas, o cruzamento das informações recolhidas e análise dos dados, ainda é realizada manualmente, não existindo o auxílio de qualquer plataforma.

Os participantes indicam que na polícia ainda não existe nenhuma ferramenta de inteligência artificial que auxilie na recolha e no processamento dos dados, o que está relacionado com a ausência de investimento do governo na modernização da polícia.

Os entrevistados indicam que existem *softwares* de análise gratuitos e disponíveis na *internet* que poderiam ser usados pela polícia, mas isso não é permitido pela Polícia de Segurança Pública, por se tratar de informação confidencial e sensível. Os polícias indicam que a introdução de dados em plataformas não verificadas e autorizadas pela Polícia de Segurança Pública pode levar à divulgação de dados de dados sensíveis e confidenciais e ao seu uso indevido por piratas informáticos.

Foi ainda pedido aos analistas para indicarem a qualidade dos recursos tecnológicos disponibilizados pela Polícia de Segurança Pública como os computadores, de modo a perceber que tipo de limitações a qualidades dos recursos técnicos existentes pode levantar à recolha e processamento de dados.

Os participantes indicaram que os recursos tecnológicos existentes distanciam-se da sofisticação das polícias internacionais e que a sua melhoria permitiria a maximização e a rentabilidade de recursos, disponibilizando mais elementos para o terreno que é, apontam os polícias, onde eles fazem efetivamente falta.

Os entrevistados referem que os analistas têm vontade de evoluir nas suas análises, através do uso de *softwares* e da inteligência artificial, mas a ausência de investimento nas tecnologias na polícia, condiciona a sua aplicabilidade. Além disso, os polícias salientam que tecnologias mais avançadas permitiriam aos analistas ocultar melhor a sua identidade e trabalhar de forma mais discreta.

Os participantes apontam que a modernização dos recursos técnicos da polícia poderia potenciar a sua capacidade preventiva, já que, por exemplo, permitiria aos analistas estabelecer um maior número de ligações entre os dados das plataformas do aquilo que os atuais recursos permitem, considerando ainda que há muito a melhorar na Polícia de Segurança Pública.

As fontes dos dados

Foi solicitado aos entrevistados que identificassem o tipo de fontes de dados que são usadas pela polícia para perceber como é que os dados analisados e processados são recolhidos.

As respostas dos participantes permitiram identificar dois tipos de fontes de informações criminais: as fontes abertas e as fontes internas. Para os polícias, as fontes internas são todas as plataformas de bases de dados que se encontram à disposição da Polícia de Segurança Pública ou partilhadas com outros órgãos de polícia criminal e cujo acesso exige credenciação prévia, ou seja, não são acessíveis a qualquer cidadão. Assim, de acordo com os polícias, a maior base de dados da Polícia de Segurança Pública, visto que, desde 2004, todos os dados que são produzidos pela ação policial, por exemplo, através de denúncias ou participações, estão aí inseridos.

Quanto às fontes abertas, os polícias definem-nas como bases de dados acessíveis a qualquer cidadão, englobando plataformas como as redes sociais, o *google* ou o *Youtube*.

Foi ainda pedido aos polícias que indicassem os problemas que cada tipo de fonte pode suscitar, de modo a compreender os desafios que os polícias enfrentam na recolha dos dados. Deste modo, quanto às fontes de dados internas, os entrevistados indicaram que a consolidação destas fontes não permite a sua evolução. Além disso, os participantes indicam que a ausência de investimento do governo na modernização das bases de dados da polícia distancia-nos da sofisticação das plataformas internacionais, o que pode também condicionar o compartilhamento de dados entre agências.

No que respeita às fontes abertas, os polícias apontam a necessidade de cruzar a informação recolhida de bases de dados abertas com dados inseridos em plataformas institucionais, a fim de apurar a sua veracidade, visto que os dados que se encontram em plataformas livres como

as redes sociais podem não corresponder à realidade e podem levar a erros de interpretação. Assim, para os polícias, ainda que todas as informações sejam úteis, devido à grande quantidade de desinformação presente na internet é importante validar os dados, através do cruzamento de várias fontes, para podermos analisá-los e extrair conhecimento.

Os entrevistados apontam ainda que o acesso às fontes abertas é limitado, isto porque os analistas só podem recolher informação de fontes de dados abertas autorizadas. De acordo com os polícias, o acesso a determinados sites é bloqueado pela instituição Polícia de Segurança Pública, o que condiciona a recolha de informação que seria relevante para o caso em estudo.

Deste modo, embora, os participantes apontem os riscos do uso de cada tipo de fontes de dados, consideram que todas fontes são interessantes de ser trabalhadas.

Foi também pedido aos polícias que indicassem a frequência e a qualidade do compartilhamento, de modo a compreender como é que a partilha de dados ocorria entre agências, através de quais plataformas e que dados eram cedidos.

As respostas dos polícias permitiram perceber que o compartilhamento é uma prática importante para a evolução das informações e frequente, embora nem sempre ocorra de forma desejável.

Os entrevistados indicam que, em Portugal, os órgãos de polícia criminal partilham informações criminais, através da Plataforma Integrada de Informações Criminais, que é uma fonte interna partilhada pelos vários órgãos de polícia criminal, em que se encontram todos os dados relacionados com as investigações em curso, permitindo uma coordenação entre as várias autoridades nacionais.

No entanto, os participantes apontam também a existência de plataformas dedicadas à partilha de informações criminais com agências internacionais, como o Sistema de Informação Schengen ou o Ponto Único Contacto de Cooperação Policial Internacional, mas salientam que apenas são partilhados os dados estritamente necessários, por razões de confidencialidade.

Os polícias referem que a partilha de dados entre agências é um processo lento, não é automático, devido à infraestrutura tecnológica de quem cede e de quem recebe a informação, das próprias políticas de governo de legislação e também das relações interinstitucionais.

Deste modo, dada a necessidade da partilha de dados intra e interagências para as operações de segurança modernas, os entrevistados consideram que é essencial o investimento do governo na infraestrutura tecnológica da polícia e a partilha de informação nos moldes

definidos pela legislação que nem sempre acontece. Os polícias indicam que as agências, para ficarem com os louros do sucesso de uma investigação, não partilham toda a informação necessária quando esta lhes é pedida. Assim, de acordo com os participantes uma partilha efetiva dados seria um passo importante para o combate ao crime.

No entanto, os polícias salientam que as informações criminais diferenciam-se das informações policiais, visto que estas últimas não precisam de informação que seja sustentada como prova e que esteja balizada por um juíz. De acordo com os participantes, nas informações policiais, os analistas podem fazer induções, mas nas informações criminais não.

Em termos de informações policiais, os participantes referem que partilha de informações essenciais para todas as unidades é realizada em reuniões semanais entre o departamento de informações policiais e o Serviço de Informações Secretas, a Polícia Judiciária, a Polícia de Segurança Pública, a Guarda Nacional Republicana e a Polícia Marítima, não existindo uma base de dados de informações policiais partilhada.

Foi também pedido aos participantes que indicassem os desafios éticos, socias e legais que o uso do *big data* pela polícia pode enfrentar, de modo a compreender que riscos o uso do *big data* no despoletar e de que forma se pode prevenir.

Os polícias indicaram que o mau uso do *big data* pela polícia pode interferir negativamente com os direitos, liberdades e garantias dos cidadãos, nomeadamente com o direito à privacidade e da liberdade individual.

Os entrevistados apontam que a Polícia de Segurança Pública não pode proceder à recolha desmensurada de dados sobre os cidadãos, porque isto não se encontra previsto na lei. De acordo com polícias, a recolha, a análise e o processamento de dados encontram-se previstos na lei e, por isso, obedecem a quadro legal, do qual não podem descurar.

Deste modo, os polícias referem que os analistas não podem realizar uma recolha de dados indiscriminada, analisá-los e prever crimes. Segundo os participantes, os polícias não podem espiar a totalidade da sociedade, incluindo pessoas idóneas, procurando prevenir crime, porque os cidadãos têm direito à sua privacidade e liberdade individual.

Além disso, os polícias salientam que, embora a polícia possa realizar análises em rede, com o objetivo de obter mais informação sobre a rede de contactos, hábitos e as rotinas de um suspeito, todos estes dados recolhidos são enquadrados legalmente, ou seja, a atuação da polícia está prevista na lei, a fim de prevenir uma recolha de dados que não respeite os direitos fundamentais dos cidadãos.

Os polícias apontam ainda a necessidade da validação dos dados antes de introduzi-los nas bases de dados da polícia, isto para a informação que é recolhida, como para a informação que é partilhada por outra entidade. Os entrevistados apontam que, mesmo que o pedido de partilha de informação seja realizado no âmbito de um processo de investigação de um crime, a informação deve ser validada, isto porque um dado errado, tal como referido pelos polícias, pode contribuir para a acusação de um inocente.

Os entrevistados referem também que os algoritmos não são 100% fiáveis, uma vez que a recolha e introdução dos dados no sistema é realizada por humanos que são seres naturalmente tendenciosos. Assim, de acordo com os participantes, os dados também podem seguir tendências que levam a enviesamentos do algoritmo.

Além disso, os participantes indicam que a recolha de dados em fontes como a *internet* e as redes socias podem levar, caso não haja uma prévia validação dos dados, à introdução de dados errados nas plataformas da polícia, isto porque cada um coloca o que quiser na *internet*, independentemente de ser verdade ou mentira. Mais se acrescenta, que os entrevistados alertam para o conteúdo de desinformação presente na *internet* e potenciado pela inteligência artificial. De acordo com os polícias, a inteligência artificial veio tornar mais difícil a tarefa de distinguir o que é verdade ou não, sendo necessário cada vez mais consciencializar os analistas da necessidade da validação dos dados antes da sua introdução nas bases de dados.

Os polícias indicam ainda que os cidadãos devem estar conscientes de que os dados que são divulgados na *internet*, nomeadamente nas redes sociais, podem ser usados pela polícia para a investigação de um crime, não considerando que a recolha de dados nas redes sociais pela polícia afete negativamente os direitos fundamentais do cidadão, porque além disto se encontrar enquadrado legalmente, trata-se, segundo os entrevistados, de falta de literacia do cidadão em perceber que os dados colocados nas redes sociais ou qualquer outra fonte aberta passam a circular livremente na *internet* e qualquer pessoa pode utilizá-los para os mais diversos fins. Assim, os polícias consideram que é essencial que os cidadãos percebam que a única forma dos nossos dados não serem usados para fins que não queremos, é não divulgá-los e protegê-los.

Os entrevistas consideram ainda que a monotorização das redes sociais feita pela polícia é importante para compreender a evolução dos crimes cibernéticos.

Os participantes que trabalham com informações policiais apontam que a sua área de trabalho é cinzenta, na medida em que atuam antes do crime ocorrer, ou seja, apesar de ainda

não existirem criminosos, há um espaço na lei que permite aos analistas que recolham e analisem dados para prevenir crimes e direcionar recursos técnicos e humanos.

Assim, os entrevistados referem que a formação é muito importante para a sensibilização dos polícias para os riscos éticos, sociais e legais que o uso do *big data* pode apresentar, permitindo-os estar conscientes da necessidade de atuarem dentro da legalidade e das consequências que podem resultar no caso dos direitos fundamentais dos cidadãos não serem protegidos. Além disso, os polícias consideram que a formação é também essencial para prevenir erros e o uso indevido do *big data.*

Os entrevistados salientam que a polícia é alvo de um escrutínio constante, e que a sua atuação tem de ser rigorosa e transparente

PARTE IV – ESTUDO EMPÍRICO (DISCUSSÃO DOS RESULTADOS)

1. Discussão dos resultados

O presente estudo tem como objetivo compreender as perspetivas e expectativas dos polícias sobre o uso do *big data* no policiamento, nomeadamente entender os riscos e benefícios que os polícias identificam no uso do *big data* na investigação e prevenção criminal, que tipo de formação possuem os analistas, que tipo de técnicas são usadas para a recolha e análise dos dados, que tipo de fontes são usadas e como é a sua qualidade e que desafios éticos, legais e sociais são identificados pelos polícias no uso do *big data* nas suas atividades profissionais. Assim, o estudo procura identificar as necessidades e os desafios sentidos pelos polícias no uso do *big data* no policiamento, de modo a procurar perceber o que é preciso fazer para diminuir os entraves ao uso do *big data* na investigação e prevenção criminal.

Inicialmente, importa referir que os resultados obtidos podem ser influenciados pelas limitações do estudo, nomeadamente o facto dos elementos da amostra pertencerem todos à mesma instituição da polícia, isto porque os resultados do estudo limitam-se às perceções e necessidades dos profissionais da Polícia de Segurança Pública e não permitem aceder às perspetivas dos profissionais de outras autoridades policias com a Polícia Judiciária, por exemplo. Além disso, a ausência de estudos sobre as perceções dos polícias do uso do *big data* na prevenção e investigação criminal no contexto português, dificulta a comparação dos resultados obtidos com outros estudos empíricos. No entanto, por outro lado, este estudo pode ser um contributo positivo para a literatura científica sobre a matéria e para o desenvolvimento de investigações futuras.

Quanto às respostas dos entrevistados sobre a definição do *big data*, estas permitiram perceber que a definição de *big data* apresentada pelos polícias é concordante com as definições encontradas na literatura científica. Assim, tal como definido, Favaretto et al.(2019), os entrevistados definem o *big data* como um grande conjunto de dados que são recolhidos e analisados para extrair informação que oriente/ informe. Ou seja, no mesmo sentido que Ridgeway (2018), para os participantes, o extenso volume dos dados é um dos principais aspetos que define o *big data*.

No entanto, as definições apresentadas pelos polícias sobre o *big data* mencionam também os outros dois aspetos que caracterizam o *big data* indicados por Ridgeway (2018), nomeadamente a variedade e a velocidade. Deste modo, os autores e os entrevistados, definem o *big data* como um grande conjunto de dados variados e que são processados rapidamente.

De acordo com os participantes e conforme indicado por Boyd e Crawford (2012), a velocidade depende da utilização de tecnologias na análise e processamento dos dados

recolhidos. Assim, como definido por Babuta (2017), os polícias apontam que o *big data* consiste numa grande quantidade de dados que são analisados, através de *softwares*.

Quando questionados sobre os benefícios do uso de *big data* na polícia, os participantes consideram, conforme apresentado por Chi (2019) que a análise das grandes quantidades de dados recolhidos permite a interpretação de informações sociais, auxiliando os líderes na alocação de recursos e no planeamento estratégico e operacional. Ou seja, para os polícias, o *big data*, como apontado por Ali (2015), consiste num conjunto de dados, cujo a análise e o processamento permitem extrair informação que orienta as decisões dos líderes para melhorar o policiamento.

Assim, segundo os polícias, a análise e o processamento dos dados recolhidos permite detetar padrões nos dados, identificando que tipo crimes são cometidos, por quem, como, quando, onde e porquê, e orientar as medidas táticas e estratégicas e o direcionamento de recursos técnicos e humanos (Neiva, 2021).

É importante salientar que as respostas obtidas quanto aos benefícios do uso do *big data* na polícia não se diferenciaram entre participantes com cargos diferentes. Na literatura científica, os estudos indicam que os líderes, nomeadamente comandantes da polícia de idade mais avançada, não consideram as informações obtidas da análise dos dados nas suas decisões (Burcher & Whelan, 2018; Cope, 2004; Sanders et al., 2015), sendo que isto cria um clima de desconfiança entre analistas e líderes. No entanto, a análise das entrevistas não permitiu concluir resultados semelhantes aos achados da literatura, na medida em que os comandantes, os analistas e os agentes apontaram contributos positivos do uso do *big data* no policiamento.

No que respeita à formação dos analistas, os polícias indicaram que estes profissionais possuíam cursos em tecnologias de informação e de análise, de modo a conseguirem apresentar a informação obtida da análise e processamento dos dados recolhidos aos comandantes para, como definido por Ratcliffe (2003) e Walsh (2011), orientar as suas decisões.

No entanto, os entrevistados apontaram que a formação dada pela instituição da Polícia de Segurança Pública não é suficiente para responder às necessidades profissionais dos analistas, não se seguindo uma das recomendações propostas pela *International Association of Chiefs of Police* que é o investimento em formação dos analistas (Peterson, 2005). Mais se acrescenta que os polícias indicam a necessidade formativa dos analistas nas áreas do cibercrime e dos direitos humanos, sensibilizando os profissionais para os erros e enviesamentos dos dados (Brayne, 2017; Burcher & Whelan, 2018). Por exemplo, a sua

sensibilização é importante para prevenirem enviesamentos dos algoritmos que resultam da inserção no sistema de dados tendenciosos (Boyd & Crawford, 2012).

No que respeita à formação dos analistas, os polícias referem que estes profissionais possuem formação nas áreas das tecnologias e da análise fornecidas pela instituição da Polícia de Segurança Pública, visto que, como mencionado por Cope (2004), é importante que o analista saiba interpretar a informação extraída dos dados e consiga apresentá-la ao comandante, de modo a orientar as suas decisões.

No entanto, os entrevistados indicam que a formação dada pela instituição da Polícia de Segurança Pública é insuficiente, nomeadamente nas áreas do cibercrime e dos direitos humanos, não somente para o acompanhamento da evolução da cibercriminalidade, mas para a sensibilização dos analistas para os riscos que o uso indevido do *big data* pode apresentar para os direitos, liberdades e garantias dos cidadãos (Wout et al., 2022).

Os entrevistados apontaram ainda que a análise e o processamento dos dados, à semelhança do estudo de Burcher & Whelan (2018), é limitada pelos equipamentos tecnológicos disponibilizados pela polícia. Os polícias referem que a análise dos dados ainda é muito manual, devido à ausência de recursos tecnológicos com capacidade para suportar a utilização de *softwares* mais sofisticados e análises mais avançadas (Burcher & Whelan, 2018)

Neste sentido, os entrevistados indicam que o auxílio de tecnologias na análise e no processamento dos dados como a inteligência artificial permitiriam extrair mais informação pela densificação do cruzamento dos dados, e a rentabilização dos recursos pelo direcionamento de mais profissionais para o terreno. Assim, tal como referido por L´heureux et al. (2017), os polícias consideram que a inteligência artificial contribui para o melhoramento do policiamento.

No entanto, os participantes salientam que na análise e no processamento dos dados, apenas podem ser usadas pelos analistas, as técnicas oficiais, ou seja, aquelas que são autorizadas pela Polícia de Segurança Pública, isto porque, de acordo com os polícias, a inserção de dados sensíveis numa plataforma pirata pode colocar em causa a confidencialidade das informações e a segurança dos cidadãos, sendo que Wout et al. (2021) consideram que o uso de tecnologias não pode afetar negativamente os direitos, liberdades e garantias dos cidadãos, ainda que por razões de segurança.

Deste modo, os polícias salientam a necessidade de investimento do governo nos recursos técnicos disponibilizadas à Polícia de Segurança Pública, uma vez que segundo Chan e Moses (2017), a ausência de recursos tecnológicos ajustados pode criar resistências na

utilização do *big data* pela polícia e pode levar à cristalização dos sistemas de informação (Pereira, 2019).

No âmbito das fontes de dados, os polícias salientaram que a recolha de dados é enquadrada legalmente, respeitando os direitos fundamentais dos cidadãos, não se podendo recolher dados indiscriminadamente de todos os cidadãos. Além disso, os profissionais indicam também que na recolha de dados devem ser utilizadas várias fontes, de modo a prevenir a introdução de informações erradas nas plataformas da polícia, que segundo Burcher & Whelan, 2018, afetam negativamente a qualidade da análise dos dados.

Os polícias indicam ainda que os analistas só podem usar as fontes de dados, internas ou abertas, devidamente autorizadas, mas que mesmo estas podem apresentar erros e enviesamentos que devem ser considerados pelos profissionais. Assim, os polícias apontam que o uso de fontes abertas como as redes sociais, o *google* ou o *Youtub*e podem levar à recolha de dados errados (Burcher e Whelan, 2018), uma vez que qualquer pessoa pode publicar qualquer coisa, sendo para isso necessária a validação dos dados antes da sua inserção nas bases de dados.

No entanto, apesar dos riscos, os entrevistados consideram que a monotorização das redes sociais pela polícia é uma tarefa importante, na medida em que permitecompreender o mundo cibernético, e que se encontra legalmente prevista na lei portuguesa, não afetando negativamente o direito à privacidade e liberdade individual dos cidadãos (Vermeulen & Lievens, 2017).

Além disso, os participantes indicam que a monitorização das redes sociais de elementos pertencentes à rede de contactos do suspeito, é uma prática policial enquadrada na lei portuguesa e que não atenta a voluntariedade da cedência dos dados, como sugerido por Bauman et al. (2014). Os polícias apontam que esta é uma questão relacionada com a falta de literacia dos cidadãos, e que a sua ação, contrariamente ao que é referido por Lyon (2014), não fragiliza a voluntariedade da cedência de dados, porque os cidadãos devem estar conscientes que qualquer informação que é divulgada numa plataforma social, pode ser usada por qualquer pessoa para qualquer fim, incluindo para a identificação de suspeitos pela polícia.

No que respeita ao compartilhamento, os polícias consideram que esta é uma prática frequente, ainda que não ocorra como desejado (Cope, 2004; Sanders et al., 2015), isto porque o processo de partilha de dados entre agências é lento, sendo que os motivos se relacionam com os quadros legislativos e princípios de governação, as infraestruturas tecnológicas e os imperativos e princípio organizacionais de cada país (Neiva, Granja e

Machado, 2002). Por exemplo, a ausência de recurso tecnológicos indicada pelos polícias pode condicionar o compartilhamento de dados entre a Polícia de Segurança Pública e outras agências.

Além disso, de acordo com os participantes e como referido por Sanders et al. (2015), o compartilhamento também parece ser condicionado pela vontade de todas as agências em serem responsáveis por uma grande deteção, o que dificulta a partilha de dados.

Deste modo, de acordo com os achados da literatura científica e as respostas dadas pelos polícias durante as entrevistas, é essencial que o governo invista na formação e nos recursos técnicos disponibilizados aos profissionais, isto porque a formação é importante para o acompanhamento da evolução do crime pelos polícias, para sensibilização dos analistas para os riscos que o *big data* pode apresentar para os direitos fundamentais dos cidadãos e para a prevenção de erros e enviesamentos dos dados que afetam negativamente o policiamento, e os recursos técnicos permitem a análise e o processamento dos dados mais aprofundada, um melhor compartilhamento dos dados entre agências, um maior conhecimento do crime e o direcionamento de mais polícias para o terreno. O investimento na formação e nos recursos técnicos da polícia pode diminuir as resistências ao uso do *big data* pelos polícias (Chan & Moses, 2017) e melhorar o policiamento (Ali, 2015).

2. Considerações finais

O presente estudo tem como objetivo explorar e compreender as perspetivas e expectativas dos polícias sobre o uso do *big data* na prevenção e investigação criminal, uma vez que, como apresentado por Neiva (2019), as perceções dos profissionais podem encorajar ou desencorajar a utilização desta ferramenta, sendo que estas podem ser influenciadas pelos quadros legislativos e princípios de governação, as infraestruturas tecnológicas e os imperativos e os princípios organizacionais de cada país (Burcher & Whelan, 2018, Cope, 2004, Neiva, Granja e Machado, 2022, & Sanders et al., 2015), mas também pelos desafios éticos, sociais e legais que o seu uso pela polícia pode enfrentar (Wout et al., 2021), afetando negativamente a relação de confiança entre cidadãos e polícias

Deste modo, dada a ausência de estudos empíricos sobre esta matéria, o presente estudo assentou em 6 entrevistas a profissionais da Polícia de Segurança Pública, nomeadamente da Divisão de Investigação Criminal e do Núcleo de Informações do Comando Metropolitano da Polícia de Segurança Pública do Porto, com cargos distintos, mais especificamente 1 comandante, 1 analista e 1 agente principal de cada uma das divisões indicadas.

Os dados recolhidos durante as entrevistas foram analisados pelo método da análise temática, seguindo as orientações de Braun e Clarke (2006), e baseou-se em 6 fases distintas, nomeadamente a familiarização dos dados, a codificação dos dados, a organização dos códigos, a refinação dos temas, a revisão dos temas e a análise e redação dos resultados.

A análise das respostas apresentadas pelos polícias permitiram compreender, ainda que os profissionais da Polícia de Segurança Pública, nomeadamente os analistas, se encontrem aptos e possuam vontade para realizar análises mais avançadas dos dados com recurso a *softwares* mais sofisticados e progredirem na obtenção de conhecimento sobre novos fenómenos criminais e novas tecnologias, os recursos técnicos e a oferta formativa disponibilizados pela instituição Polícia de Segurança Pública não permite satisfazer as necessidades sentidas pelos polícias, o que, de acordo com Burcher & Whelan (2018) e Cope (2004), pode condicionar a análise e o processamento dos dados recolhidos e comprometer o papel orientador do produto *intelligence* nas decisões dos líderes.

Uma das práticas mais afetadas negativamente pela ausência de tecnologias evoluídas é o compartilhamento de dados entre agências, que também parece ser limitado, segundo os participantes e o estudo de Sanders et al. (2015), pela vontade das agências em ficarem com os louros de uma investigação bem-sucedida. Além disso, em conformidade com Neiva, Granja e Machado (2022), os polícias apontaram que as diferenças entre as legislações e os princípios institucionais de cada país podem também afetar negativamente o compartilhamento de dados, as técnicas usadas para a análise e processamento dos dados e as fontes de dados autorizadas.

Contudo, para os entrevistados, a legislação é essencial para o enquadramento legal e regulação da atividade dos analistas, de modo a proteger e salvaguardar os direitos fundamentais dos cidadãos. Como indicado por Wout et al. (2021), os direitos, as liberdades e garantias dos cidadãos não podem afetadas negativamente, ainda que por razões securitárias, exceto os casos em que a lei assim o prevê.

A formação dos analistas também foi um ponto primordial nas repostas dos polícias, nomeadamente no que concerne à prevenção dos desafios éticos que o uso mau do *big data* e os enviesamentos do algoritmo podem enfrentar relativamente à proteção de dados e dos direitos fundamentais dos cidadãos (Brayne, 2017).

Para os polícias, a formação permite a consciencialização e sensibilização dos profissionais para os riscos que o uso mau do *big data* pode suscitar e para a necessidade de agir dentro do quadro legal previsto, a fim de salvaguardar o direito à privacidade e liberdade individual dos cidadãos.

Neste sentido, a Polícia Segurança Pública carece de investimento pelo governo nos recursos tecnológicos e na formação contínua disponibilizada aos polícias, contrariamente ao recomendado pelo *International Association of Chiefs of Police* (Peterson, 2005), que é essencial para que as necessidades identificadas pelos profissionais possam ser colmatadas e o policiamento melhore, permitindo análises mais complexas dos dados, um maior conhecimento do crime, um melhor policiamento preditivo e um melhor direcionamento dos recursos técnicos e humanos.

Embora o presente estudo apresente limitações como a concentração exclusiva nas perceções dos profissionais da Polícia de Segurança Pública, não se explorando e comparando as suas perspetivas e expectativas com polícias de outras instituições, e a ausência de estudos empíricos sobre a matéria, não permitindo a comparação dos resultados obtidos e a densificação da discussão dos resultados, este trabalho pode ser um contributo positivo para a literatura científica, encorajando que investigações futuras procurem compreender o uso do *big data* noutras instituições da polícia, por exemplo na Polícia Judiciária, a fim de explorar as perceções dos polícias, os benefícios e os riscos da sua utilização e as ferramentas e fontes de dados usadas.

REFERÊNCIAS

Ali, B. (2015). Big Data-Driven Smart Policing: Big Data Based Patrol Car Dispatching. *Journal of Geotechnical and Transportation Engineering, 1*(2), 49-52. https://jgtte.com/issues/2/Issue%202%20-%204.pdf

Alshenqeeti, H. (2014) Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research, 3*(1), 39-45. https://doi.org/10.5430/elr.v3n1p39

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

Araújo, V., Zullo, B, & Torres, M. (2020). Big Data, algoritmos e inteligência artificial na Administração Pública: reflexões para a sua utilização em um ambiente democrático. *Revista de Direito Administrativo & Constitucional, 20* (80), 241-261. https://doi.org/10.21056/aec.v20i80.1219

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/

Bartlett, A., Lewis, J., Reyes-Galindo, L., & Stephens, N. (2018). The locus of legitimate interpretationin Big Data sciences: Lessons for computational social science from-omic biology and high-energy physics. *Big Data & Society, 5*(1), 1-15. https://doi.org/10.1177/2053951718768831

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

Belur, J., & Johnson, S. (2018). Is crime analysis at the heart of policing practice? A case study. *Policing and Society, 28*(7), 768-786. https://doi.org/10.1080/10439463.2016.1262364

Bench-Capon, T. (1990). *Knowledge Representation: An Approach to Artificial Intelligence.* Academic Press.

Boyatzis, R. (1998). *Transforming qualitative information: Thematic analysis and code development.* Sage.

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), https://doi.org/10.1177%2F0003122417725865 977-1008.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology

Burcher, M., & Whelan, C. (2018). Intelligence-led policing in practice: Reflections from intelligence analysts. *Police Quarterly, 0*(0), 1–22. https://doi.org/10.1177/1098611118796890

Bureau of Justice Assistance (2003). *National criminal intelligence sharing plan.* U.S. Department of Justice. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/national_criminal_intelligence_sharing_plan.pdf

Carter, D. (2004). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies* (3a ed). Institute for Intergovernmental Research. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Law_Enforcement_Intelligence_Guide_508.pdf

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

Chi, X. (2019). Innovation of Police Model Under the Background of Big Data. *Advances in Social Science, Education and Humanities Research, 375,* 28-31. https://www.atlantis-press.com/proceedings/ssmi-19/125925360

Comissão Europeia. (2021). Regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial) e altera determinados atos legislativos da união. COM (2021) 206 final. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206

Cope, N. (2004). Intelligence led policing or policing led intelligence? *British Journal of Criminology, 44* (2),188-203. https://doi.org/10.1093/bjc/44.2.188

Costa, R. (2004). Sociedade de controle. *São Paulo Em Perspetiva, 18*(1), 161-167. https://www.scielo.br/j/spp/a/ZrkVhBTNkzkJr9jVw6TygVC/?format=pdf&lang=pt

Cozman, F. (2012). O futuro da (pesquisa em) inteligência artificial: algumas direções. *Revista USP, 124,* 11-20. https://doi.org/10.11606/issn.2316-9036.v0i124p11-20

Eberendu (2016). Unstructured Data: an overview of the data of Big Data. *International Journal of Computer Trends and Technology 38* (1), 46-50. https://www.researchgate.net/publication/309393428_Unstructured_Data_an_overview_of_the_data_of_Big_Data

Ericson, R., & Haggerty, K. (1997). *Policing the Risk Society.* Toronto & Buffalo: University of Toronto Press.

Favaretto, M, Clercq, E., & Elger, B. (2019). Big Data and discrimination: perils, promises and solutions. *A systematic review. Journal of Big Data, 6* (12), 2-27. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0177-4

Fernandes, L. (2014). *Intelligence e Segurança Interna* (Master's thesis, Instituto Superior de Ciências Policiais e Segurança Interna). Repositório Comum. https://comum.rcaap.pt/bitstream/10400.26/35125/1/INTELI~1.PDF

Fouché, G., & Langit, L. (2011). *Foundations of SQL server 2008 R2 business intelligen*ce (2nd ed.). Apress. https://www.abebooks.com/9781430233244/Foundations-SQL-Server-2008-Business-1430233249/plp

Fuentes, J. (2006). *Practical Guide to Intelligence-Led Policing*. New Jersey State Police. https://nj.gov/njsp/divorg/invest/pdf/njsp_ilpguide_010907.pdf

Hale, C., Heaton, R., & Uglow, S. (2004). Uniform styles? Aspects of police centralization in England Wales. *Policing and Society, 14*(4), 291-312. https://doi.org/10.1080/1043946042000286038

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

Kent, S. (1967). *Informações estratégicas*. Bibliex. https://pt.scribd.com/document/402503158/Informacoes-Estrategicas-Sherman-Kent-pdf

Kvale, S. (1996). *Interviews: An Introduction to Qualitative Research Interviewing*. Sage.

Lee, K. (2018). *As Superpotências da Inteligência Artificial: A China, Silicon Valley e a nova ordem mundial*. Relógio D'Água Editores. https://bibliografia.bnportugal.gov.pt/bnp/bnp.exe/registo?2025684

L'heureux, A., Grolinger, K., Elyamany, H., & Capretz, M. (2017). Machine learning with big data: challenges and approaches. *IEEE Access (99)* 1, 1-22. https://www.researchgate.net/publication/316448042_Machine_Learning_With_Big_Data_Challenges_and_Approaches

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1* (1) 1–13. https://www.researchgate.net/publication/266064951_Surveillance_Snowden_and_Big_Data

Machado, C. (2004). *Crime e insegurança. Discursos do medo, imagens do Outro.* Editorial Notícias.

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* (2014). https://doi.org/10.1093/bjc/azz057

McGarrell, E., Freilich, J., & Chermak, S. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice, 23*(2), 142-158. https://doi.org/10.1177/1043986207301363

Mejias, U., & Couldry, N. (2019). Datafication. *Internet Policy Review, 8* (4), 1-10. https://doi.org/10.14763/2019.4.1428

Morelato, M., Beavis A., Tahtouh, M., Ribaux, O., Kirkbride, P., & Roux, C. (2013). The use of forensic case data in intelligence-led policing: The example of drug profiling. *Forensic Science International, 226* (3), 1-9. https://doi.org/10.1016/j.forsciint.2013.01.003

Neiva, L. (2019). *Big Data na investigação criminal: previsão do risco, vigilância e expectativas sociais na União Europeia* (Master's thesis, Universidade do Minho). Repositório da Universidade do Minho. http://repositorium.sdum.uminho.pt/handle/1822/61235

Neiva, L. (2021). Big data e vigilância policial: Desafios éticos, legais e sociais. In H. Machado (Ed.), *Crime e tecnologia: Desafios culturais e políticos para a Europa* (pp. 65-89). Edições Afrontamento.

Neiva, L., Granja, R., & Machado, H. (2022). Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union. *Policing and Society, 32*(10), 1167-1179. https://doi.org/10.1080/10439463.2022.2029433

Neto, V., Bonacelli, M., Pacheco, C. (2020). O Sistema Tecnológico Digital: inteligência artificial, computação em nuvem e Big Data. *Revista Brasileira de Inovação, 19*, 1-31. https://doi.org/10.20396/rbi.v19i0.8658756

Patton, M. (1991). *Qualitative evaluation and research methods* (3nd ed). Sage. https://aulasvirtuales.wordpress.com/wp-content/uploads/2014/02/qualitative-research-evaluation-methods-by-michael-patton.pdf

Patton, M. (2015). *Qualitative evaluation and research methods* (4nd ed.). Sage.

Pereira, M. (2019). *Big Data: O caso do Sistema Estratégico de Informação, Gestão e Controlo Operacional da Polícia de Segurança Pública* (Master's thesis, Instituto Superior de Ciências Policiais e Segurança Interna). Repositório Comum. https://comum.rcaap.pt/bitstream/10400.26/30342/1/Disserta%c3%a7%c3%a3o-de-Mestrado-156105-vers%c3%a3o-final-NOV19.pdf

Peterson, M. (2005). *Intelligence-Led Policing: The New Intelligence Architecture.* Bureau of Justice Assistance. https://www.policinginstitute.org/publication/intelligence-led-policing-the-new-intelligence-architecture/

Petintseva, O., Faria, R., & Eski, Y. (2020). *Interviewing elites, experts and the powerful in criminology*. Springer

Ratcliffe, J. (2003). Intelligence-led Policing. *Trends and Issues in Crime and Criminal Justice n crime and criminal justice, 248,* 1-6. https://www.aic.gov.au/publications/tandi/tandi248

Ratcliffe, J. (2008). *Intelligence-Led Policing.* Willan. https://doi.org/10.4324/9780203118245

Ratcliffe, J., & Guidetti, R. (2008). State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management. 31* (1), 109-128. https://www.researchgate.net/publication/242021222_State_police_investigative_structure_and_the_adoption_of_intelligence-led_policing

Richards, J. (2012). Intelligence Dilemma? Contemporary Counterterrorism in a Liberal Democracy. *Intelligence and National Security, 27*(5), 761-780. https://doi.org/10.1080/02684527.2012.708528

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

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163-180. https://www-public.imtbs-tsp.eu/~gibson/Teaching/Teaching-ReadingMaterial/Rowley06.pdf

Sanders, C., & Sheptycki, J. (2017). Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. *Crime, Law and Social Change. An Interdisciplinary Journal, 68*(1), 1–15. https://link.springer.com/article/10.1007/s10611-016-9678-7

Sanders, C., Weston, C., & Schott, N. (2015). Police innovations 'secret squirrels' and accountabilliy: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology, 55*(4), 711-729. https://www.jstor.org/stable/43819547

Scott, M. (2000). *Problem Oriented Policing: Reflections on The First 20 Years.* U.S. Department of Justice. https://popcenter.asu.edu/sites/default/files/library/reading/pdfs/Reflections-2.pdf

Shermer, B. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review, 27* (1), 45-52. https://www.sciencedirect.com/science/article/abs/pii/S0267364910001767

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

Souza, L. (2019). Pesquisa com análise qualitativa de dados: conhecendo a Análise Temática. *Arquivos Brasileiros de Psicologia, 71* (2), 51-67. http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S180952672019000200005

Taulli, T. (2019). *Introdução à Inteligência Artificial: uma abordagem não técnica.* Novatec Editora.

Taylor, R., & Russell, A. (2012). The failure of police 'fusion' centers and the concept of a national intelligence sharing plan. *Police Practice and Research: An International Journal, 13*(2), 184-200. https://doi.org/10.1080/15614263.2011.581448

Telles, P. (2021). Inteligência artificial e polícia preditiva: limites e possibilidades. *Boletim Científico ESMPU, 20* (57), 247-263. https://pt.scribd.com/document/627561245/10-Inteligencia-artificial

Tsai, C., Lai, C., Chao, H., & Vasilakos, A. (2015). Big data analytics: a survey. *Journal of Big Data*, *21*(2), 1-32. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-015-0030-3

Tuckett, A. (2005). Applying thematic analysis theory to practice: A researcher's experience. *Contemporary Nurse, 19*(2), 75-87. https://www.researchgate.net/publication/7597116_Applying_Thematic_Analysis_Theory_to_Practice_a_researcher's_experience

Vermeulen, G., & Lievens, E. (2017). *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data*. (1nd ed). Maklu. https://www.edps.europa.eu/sites/default/files/publication/171218_wiewiorowski_data_protection_and_privacy_under_pressure_en.pdf

Ylijoki, O., & Porras, J. (2016). Perspectives to Definition of Big Data: A Mapping Study and Discussion. *Journal of Innovation Management*,*4*(1), 69-91. https://doi.org/10.24840/2183-0606_004.001_0006

Walsh, P. (2011). *Intelligence and intelligence analysis*. (1nd ed). Willan. https://doi.org/10.4324/9780203815939

Wiggett, A., Walters, A., O'Hanlon, L., & Ritchie, F. (2003) Forensic Science Society. *Sci Justice, 43*(2), 109-18. https://pubmed.ncbi.nlm.nih.gov/12879574/

Wout, E., Pieringer, C., Irribarra, D., Asahi, K., & Larroulet, P. (2021) Machine learning for policing: a case study on arrests in Chile. *Policing and Society, 31*(9), 1036-1050. https://doi.org/10.1080/10439463.2020.1779270

Zakir, J., Seymour, T., & Berg, K. (2015). Big Data analytics. *Issues in Information Systems,16* (2), 81-90. https://doi.org/10.48009/2_iis_2015_81-90

ANEXOS

Anexo A- Pedido de autorização

PEDIDO DE AUTORIZAÇÃO À INSTITUIÇÃO PARA A REALIZAÇÃO DE UM PROJETO DE INVESTIGAÇÃO

Exmos. Sr. Diretor Nacional da Polícia de Segurança Pública e Sr. Comandante do Comando Metropolitano do Porto da Polícia de Segurança Pública
Assunto: Pedido de autorização para a realização de um projeto de investigação
Porto, 02 de janeiro de 2024

Eu, Carolina Gomes Glória, venho por este meio solicitar a colaboração da vossa prestigiada instituição para recolha de dados que servem o Projeto "As perspetivas dos polícias sobre a aplicação do *big data* no policiamento", que está a ser desenvolvido no âmbito do Mestrado de Criminologia da Faculdade de Direito da Universidade do Porto, sob orientação da Professora Doutora Carla Cardoso e que tem por objetivo aceder e compreender as perspetivas e expectativas dos polícias sobre o uso do *big data* no policiamento.
A amostra do estudo assenta em 6 polícias da Polícia de Segurança Pública, nomeadamente 3 profissionais da Divisão de Investigação Criminal e do Núcleo de Informações do Comando Metropolitano do Porto da Polícia de Segurança Pública, com cargos distintos, mais especificamente 1 comandante, 1 analista e 1 agente principal de cada divisão referida. Todos os participantes dos estudos devem possuir conhecimento e experiência sobre o objeto de estudo.
As entrevistas serão realizadas num lugar a acordar com o entrevistado e terão a duração média de 30 minutos.
Em anexo, segue, ainda, o consentimento informado, onde se esclarece os objetivos do estudo e que a sua participação no mesmo é livre, voluntária e informada. São ainda esclarecidos sobre a possibilidade de desistir em qualquer momento e informa-se que os dados recolhidos durante as entrevistas serão confidenciais e anonimizados, servindo somente os fins do estudo. Os dados serão protegidos num local seguro, ao qual só eu e a minha orientadora teremos acesso, sendo destruídos quando a investigação estiver finalizada.
É ainda solicitada autorização para a gravação em áudio das entrevistas, de modo a facilitar a recolha e análise dos dados, que serão destruídas, após as transcrições.
Todos os participantes devem assinar o consentimento informado para a realização das entrevistas.

Encontro-me disponível para qualquer esclarecimento adicional, através do email up201807889@up.pt.

Agradecemos a vossa colaboração.

Anexo B – Consentimento informado

PROTOCOLO DE CONSENTIMENTO DE PARTICIPAÇÃO NUMA ENTREVISTA NO ÂMBITO DE UM PROJETO DE INVESTIGAÇÃO

Convidamo-lo a ser entrevistado para o Projeto "As perspetivas dos polícias sobre a aplicação do *big data* no policiamento", que está a ser desenvolvido no âmbito do Mestrado de Criminologia da Faculdade de Direito da Universidade do Porto, sob orientação da Professora Doutora Carla Cardoso e que tem por objetivo aceder e compreender às perspetivas e expectativas dos polícias sobre o uso do *big data* na prevenção e investigação criminal.

A sua participação é totalmente livre e voluntária, podendo desistir da mesma a qualquer momento ou recusar responder a qualquer pergunta.

Para facilitar a recolha e a análise da informação, pedimos a sua autorização para proceder à gravação por áudio da entrevista. A gravação será armazenada em local seguro, sem qualquer informação que permita a sua identificação, e será destruída depois da finalização deste trabalho. Note-se que o tratamento dos dados recolhidos garante o anonimato e a confidencialidade, nunca sendo feito qualquer tipo de uso que possa revelar a identidade dos participantes.

Os resultados obtidos serão usados exclusivamente para o presente estudo.

Encontro-me disponível para qualquer esclarecimento adicional, através do email up201807889@up.pt.

Agradecemos a sua participação.

Depois de ouvir as explicações acima referidas, declaro que:

i) Recebi uma cópia deste documento;

ii) Li e compreendi a informação que consta neste documento e que fui devidamente informado e esclarecido dos objetivos e das condições de participação na entrevista;

iii) Tive oportunidade de realizar perguntas e de ser esclarecido acerca de outros aspetos;

iv) Autorizo a gravação da entrevista (assinalar com x a opção) Sim [ ] Não [ ]

Data e local:

Assinatura do Participante:

Anexo C- Guião de entrevista

Dimensões	Subdimensões	Questões-exemplo
Conhecimento	Definição do big data Benefícios do uso do big data	Com base, na sua experiência, fale-me um pouco sobre a tecnologia big data? Quais os benefícios do uso da tecnologia big data no policiamento? Pode exemplificar
Atores	Identificação do papel dos analistas	Que tipo de formação têm os analistas? Que tipo de funções desempenham?
Ferramentas	Tipos de tecnologia usada Qualidade dos recursos tecnológicos disponibilizados pelas agências	Que tipo de tecnologias são utilizadas para o big data? Como descreve a qualidade dos recursos disponibilizados pela polícia?
Fontes	Fontes usadas	Que tipo de fontes são usadas pela polícia para recolher dados?

	Compartilhamento de dados	Fale-me um pouco sobre o compartilhamento de dados intra e interagências, nomeadamente quanto à sua facilidade e frequência?
	Qualidade dos dados	Fale-me um pouco sobre a qualidade dos dados existentes nas bases de dados?
	Relação entre Fontes de dados e desafios éticos sociais e legais	Quais considera serem os riscos e os perigos éticos, sociais e legais do uso do big data nas atividades da polícia? Pode exemplificar?
Direções futuras	Necessidade	Quer acrescentar alguma informação à entrevista?