ACADEMIA MILITAR

A utilização do *Data Led Policing* na prevenção criminal: Estudo de caso da República Popular da China

Aspirante de Cavalaria da GNR Miguel Jacob Sena Sardinha

Trabalho de Investigação Aplicada

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Orientadora: Major de Infantaria da GNR Adriana Filipa Gameiro Martins

Júri

Presidente: Professora Associada Ana Maria Carapelho Romão Leston Bandeira

Arguente: Capitão PILAV Tiago Carvalho

Orientadora: Major de Infantaria da GNR Adriana Filipa Gameiro Martins

Diretora de Curso: Tenente-Coronel de Cavalaria da GNR Lucília de Jesus Mendes da Silva

junho de 2025

ACADEMIA MILITAR

A utilização do *Data Led Policing* na prevenção criminal: Estudo de caso da República Popular da China

Aspirante de Cavalaria da GNR Miguel Jacob Sena Sardinha

Trabalho de Investigação Aplicada

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Orientadora: Major de Infantaria da GNR Adriana Filipa Gameiro Martins

Júri

Presidente: Professora Associada Ana Maria Carapelho Romão Leston Bandeira

Arguente: Capitão PILAV Tiago Carvalho

Orientadora: Major de Infantaria da GNR Adriana Filipa Gameiro Martins

Diretora de Curso: Tenente-Coronel de Cavalaria da GNR Lucília de Jesus Mendes da Silva

junho de 2025

EPÍGRAFE

"If You Fail to Plan, You Are Planning to Fail."

(Benjamin Franklin, 1790)

DEDICATÓRIA

A todos que ajudaram a tornar um sonho,
num plano e consequentemente numa realidade

AGRADECIMENTOS

O presente Trabalho de Investigação Aplicada representa não só a conclusão dos 5 anos em que tive a honra de estudar na Academia Militar, em que dediquei todo o meu esforço para a carreira das Armas na Guarda Nacional Republicana, que escolhi com todo o garbo, mas também o início de todo um novo ciclo. O ingresso nos quadros da Guarda como Oficial, resulta não só do meu trabalho pessoal, mas de todas as personalidades que me acompanharam e contribuíram para o meu sucesso durante este curso e até mesmo nos anos antecedentes ao mesmo. A todos esses amigos, companheiros, exemplos, bons ou maus, um sincero agradecimento por me moldarem até ao que sou hoje.

Gostaria de deixar uma palavra de agradecimento aos meus pais. Que me sirvam de exemplo nesta nova jornada, como o têm feito desde o dia em que nasci. Por um mero obrigado nunca ser suficiente, espero-vos orgulhosos pelo caminho que estou a traçar com o vosso nome.

À minha orientadora, Major GNR INF Adriana Martins, o meu pessoal agradecimento por todo o apoio durante a elaboração desta investigação. Desejo-lhe sucesso e felicidades tanto a nível pessoal como profissional.

Ao meu curso, XXX CFO GNR, pelos anos vividos nesta casa que ganhou tanto significado para todos nós. Em especial aos meus camaradas do curso de Cavalaria, Barbara Afonso, Diogo Pires e José Azevedo por todo companheirismo e amizade. Que nos mantenhamos unidos nesta jornada que agora se inicia.

Ao camarada João Borges, pela amizade e pelos momentos partilhados durante estes cinco anos de curso. Por ter feito tanto por mim, tanto dentro como fora do âmbito do curso, o meu maior obrigado.

A todos os que de uma forma ou de outra tiveram um papel preponderante neste momento em específico e que contribuíram para a concretização deste ciclo de cinco anos que se aproxima do seu términus.

Um bem-haja a todos!

RESUMO

A presente investigação analisou a utilização do modelo de *Data Led Policing* no âmbito da prevenção criminal na República Popular da China, analisando posteriormente a viabilidade e os impactos da aplicação do mesmo modelo no contexto português. A investigação, partindo da questão de partida "qual o impacto da utilização do *Data Led Policing* no âmbito da prevenção criminal na República Popular da China?", desdobrada em três questões derivadas. A primeira procurou compreender como é que o *Data Led Policing* é utilizado na RPC; a segunda explorou os contributos desse modelo para a atividade policial; e a terceira questionou de que forma o *Data Led Policing* poderia ser utilizado em Portugal. Para responder a estas questões, adotou-se uma metodologia qualitativa, assente num estudo de caso, que combinou uma revisão bibliográfica aprofundada com a realização de entrevistas semiestruturadas a dez especialistas das áreas da Administração Interna, Direito e Relações Internacionais. No domínio da prevenção criminal, o *Data Led Policing* revelou-se uma ferramenta estratégica que permite antecipar comportamentos desviantes, identificar áreas de risco e otimizar a alocação de recursos policiais. A sua lógica preditiva e orientada por dados integra-se principalmente na prevenção situacional e primária, proporcionando uma atuação mais proativa das forças de segurança. No entanto, essa eficácia preventiva está intimamente ligada ao regime político onde é aplicado, sendo que o modelo chinês privilegia a eficácia em detrimento das garantias individuais. Os resultados revelaram que o *Data Led Policing* na República Popular da China é amplamente sustentado por uma lógica de vigilância massiva e integração tecnológica, destacando-se pela recolha e processamento de *Big Data*. Entre os principais contributos identificados encontram-se o aumento da capacidade preditiva e a eficiência operacional das forças de segurança. Conclui-se que o modelo de *Data Led Policing*, tal como aplicado na República Popular da China, apresenta incompatibilidades estruturais significativas face ao enquadramento jurídico e cultural português. A eventual transposição do modelo para Portugal será necessariamente parcial, limitada à adoção tecnológica com salvaguardas legais, éticas e democráticas. A sua aplicação em regimes democráticos exige adaptação rigorosa ao respeito pelos direitos fundamentais e pelo Estado de direito.

Palavras-chave: Big Data; Data Led Policing; Portugal; Prevenção Criminal; República Popular da China.

ABSTRACT

This research examined the utilization of the Data Led Policing model within the framework of crime prevention in the People's Republic of China, subsequently assessing the feasibility and potential impacts of applying the same model in the Portuguese context. The study was guided by the central research question: “What is the impact of the use of Data Led Policing in the context of crime prevention in the People's Republic of China?”, which was further subdivided into three derivative questions. The first aimed to understand how Data Led Policing is operationalized in the People's Republic of China; the second explored the contributions of this model to police activities; and the third investigated how Data Led Policing could potentially be employed in Portugal. To address these questions, a qualitative methodology was adopted, based on a case study that combined an in-depth literature review with semi-structured interviews conducted with ten experts in the fields of Internal Administration, Law, and International Relations. In the field of crime prevention, Data Led Policing has proven to be a strategic tool for anticipating deviant behaviours, identifying high-risk areas, and optimizing the allocation of police resources. Its predictive, data-driven logic is chiefly applied to situational and primary prevention, enabling a more proactive posture by law enforcement. However, this preventive efficacy is closely tied to the political regime in which it operates, as the Chinese model privileges effectiveness over individual safeguards. The findings revealed that Data Led Policing in the People's Republic of China is predominantly underpinned by a logic of mass surveillance and technological integration, with a strong emphasis on the collection and processing of Big Data. Among the key contributions identified were the enhancement of predictive capacities and the operational efficiency of law enforcement agencies. It is concluded that the Data Led Policing model, as implemented in the People's Republic of China, presents significant structural incompatibilities with the Portuguese legal and cultural framework. Any potential transfer of the model to Portugal would necessarily be partial, limited to the adoption of technological components with legal, ethical, and democratic safeguards. Its implementation in democratic regimes requires careful adaptation to ensure compliance with fundamental rights and the rule of law.

Keywords: Big Data; Data Led Policing; Portugal; Crime Prevention; People's Republic of China.

ÍNDICE GERAL

ÍNDICE DE TABELAS

LISTA DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

Art.º		Artigo
CFO		Curso de Formação de Oficiais
CNPD		Comissão Nacional de Proteção de Dados
CRP		Constituição da República Portuguesa
DC		*Data Center*
DLP		*Data Led Policing*
FSS		Forças e Serviços de Segurança
GNR		Guarda Nacional Republicana
GSP		*Golden Shield Project*
IA		Inteligência Artificial
IJOP		*Integrated Joint Operations Plataform*
ILP		*Intelligence Led Policing*
IoT		*Internet of Things*
IWIO		*Information warfare and influence operations*
LOIC		Lei da Organização da Investigação Criminal
LPIP		Lei de Proteção de Informações Pessoais
LSE		Lei de Segurança do Estado
N. º		Número
O_E		Objetivo Específico
O_G		Objetivo Geral
OPC		Órgão de Polícia Criminal
PA		Policiamento Algorítmico
PCC		Partido Comunista Chinês

PIIC		Plataforma de Intercâmbio de Informação Criminal
PUC-CPI		Ponto Único de Contacto para a Cooperação Policial Internacional
Q_D		Questão Derivada
Q_P		Questão de Partida
RCAAP		Repositório Científico de Acesso Aberto de Portugal
RGPD		Regulamento Geral de Proteção de Dados
RPC		República Popular da China
RUSI		*Royal United Serviçe Institute*
SC		*Smart Cities*
SCS		Sistema de Crédito Social
SIIC		Sistema Integrado de Informação Criminal
SSI		Sistema de Segurança Interna
TIC		Tecnologias de Informação e Comunicação

INTRODUÇÃO

No âmbito do término do mestrado integrado de Ciências Militares, especialidade de segurança, da Academia Militar, realiza-se esta investigação cujo tema é "A utilização do *Data Led Policing* na prevenção criminal: Estudo de caso da República Popular da China".

A investigação versa essencialmente sobre a emergência de dados e tecnologias na prevenção criminal. Para tal, é necessário qualificar esta Nova Era de prevenção criminal, com uma maior panóplia de tecnologias e dados de interesse para as Forças e Serviços de Segurança como *Data Led Policing* (DLP) (Jansen, 2018).

Para compreender o DLP é vital compreender que dados se tratam quando se fala neste tópico. Entendemos assim como o conjunto de dados que são recolhidos, analisados, convertidos em algoritmos, categorizados numericamente e identificados para, posteriormente, extrair informação destes dados que capacite e oriente as políticas de combate à criminalidade (Gonçalves, 2017).

Machado (2019) destaca que o paradigma do *Big Data* permite uma análise mais aprofundada dos fenómenos criminais, possibilitando a identificação de padrões e tendências que podem ser utilizados para desenvolver estratégias mais eficazes de prevenção e combate ao crime. No entanto, também alerta para os riscos associados à utilização massiva de dados, como a potencial reprodução de desigualdades sociais e a violação de direitos fundamentais.

Segundo Braga (2019), é de extrema importância uma contínua implementação de programas de dissuasão de problemas graves de criminalidade.

Sendo a República Popular da China (RPC) uma autocracia, denota-se uma valoração da predição para um maior controlo político e da ordem social neste mesmo estado (Beraja et al., 2021). O modelo político da RPC inscreve-se inequivocamente no campo das autocracias contemporâneas, embora com características singulares que lhe conferem uma sofisticação particular. De acordo com Yang (2024), a RPC exemplifica aquilo que se designa por "Autocracia 2.0", uma forma de regime autoritário que alia a vitalidade económica, inovação tecnológica e proeminência internacional a um sistema político altamente centralizado e controlado pelo Partido Comunista Chinês (PCC).

Neste modelo, o poder político encontra-se fortemente concentrado na elite partidária, não existindo mecanismos de concorrência política significativa, liberdade de imprensa, independência judicial ou representação pluralista.

Ainda que não recorra sistematicamente à repressão violenta como forma primária de controlo, o regime exerce a sua autoridade através de instrumentos mais subtis, nomeadamente incentivos económicos, vigilância digital sofisticada e controlo ideológico sobre a sociedade. Também os índices internacionais de direitos civis e liberdades políticas colocam a RPC entre os países com menor grau de liberdade, sendo frequentemente classificada pelas organizações internacionais como um dos regimes mais restritivos em matéria de garantias individuais. Esta combinação de controlo eficaz e ausência de liberdades fundamentais consolida a natureza autoritária do regime chinês no século XXI.

A principal questão que se coloca nesta investigação é como o uso de dados eletrónicos captados ou recolhidos estando estes armazenados ou em trânsito, e de análises estatísticas contribui para a prevenção criminal na RPC. Gkougkoudis (2022) fornece uma base sólida para compreender o DLP como uma abordagem estratégica à prevenção do crime, destacando a importância de analisar dados de maneira inteligente. São explorados estudos de caso, relatórios governamentais e artigos académicos e científicos para obter uma compreensão abrangente das práticas de DLP na RPC. Os objetivos fundamentais desta investigação são fundamentalmente analisar as estratégias do DLP utilizadas na RPC para a prevenção criminal, analisar o impacto do DLP na redução da criminalidade e analisar a aplicabilidade do DLP em Portugal.

O objetivo desta investigação consiste em compreender de que forma o DLP é aplicado na antecipação e identificação de comportamentos desviantes, na deteção de áreas com maior propensão à criminalidade, incluindo no espaço ciber, e na otimização da alocação de recursos pelas FS. Deste modo, o objetivo geral (**O_G**) é: Analisar os resultados da utilização do *Data Led Policing* na Prevenção Criminal na RPC.

Esta investigação tem essencialmente dois planos que se convertem nos objetivos específicos (**O_E**) da mesma.

O primeiro O_E centra-se na perspetiva estratégica e operacional do DLP enquanto ferramenta de gestão e apoio à tomada de decisão em matéria de prevenção criminal. Este concentra-se na utilização de um policiamento orientado para os dados no que concerne à perspetiva da RPC, nomeadamente de que forma o DLP é aplicado e qual o resultado da mesma utilização. É então focado para a materialização do DLP. Esta análise acarreta alguma sensibilidade no que diz respeito à recolha, tratamento e análise dos dados obtidos.

O segundo O_E trata essencialmente de averiguar os desafios da implementação do DLP e a sua aplicabilidade em Portugal. Apresenta uma perspetiva crítica e de viabilidade no que concerne à implementação deste modelo num contexto jurídico e ético distinto.

São assim concretizados os objetivos específicos desta investigação:

- O_{E1}: Analisar o *Data Led Policing* na prevenção criminal da República Popular da China;
- O_{E2}: Analisar a aplicabilidade do *Data Led Policing* em Portugal.

Sendo que "as questões de investigação são as premissas sobre as quais se apoiam os resultados de investigação" (Fortin, 2009, p. 101), é de extrema relevância estabelecer questões de investigação concretas que conduzam a investigação de acordo com os seus objetivos. De acordo com Rosado, "é crucial proceder sempre a uma criteriosa delimitação do estudo, seja em termos de tempo, seja em termos de espaço" (2017, p. 122).

De acordo com os objetivos enunciados podemos delinear a seguinte Questão de Partida (**Q_P**): Qual o impacto da utilização do DLP, no âmbito da prevenção criminal na República Popular da China?

Esta investigação está encadeada logicamente, seguindo as normas para a redação de trabalhos finais de investigação na Academia Militar. Começa por uma revisão de literatura que aborda as principais temáticas e conceitos envolvidos na investigação.

A segunda parte da investigação é o enquadramento metodológico e trabalho de campo, em que se aborda a metodologia, métodos e materiais num primeiro ponto, passando pela apresentação, análise e discussão de resultados e finaliza concluindo a investigação, fazendo igualmente algumas considerações para trabalhos futuros.

PARTE 1 – REVISÃO DA LITERATURA

CAPÍTULO 1 – MODELOS DE POLICIAMENTO COM RECURSO A TECNOLOGIAS

O policiamento tem-se desenvolvido como resposta à evolução da sociedade e à necessidade de adaptação às novas exigências de segurança, num processo que acompanha transformações sociais, tecnológicas e políticas (Rodrigues, 2019). Esta evolução não é linear e reflete a necessidade de encontrar equilíbrios entre centralização estatal e autonomia local, de forma a assegurar a segurança e o bem-estar da comunidade, respeitando os direitos fundamentais (Rodrigues, 2019). Os modelos de policiamento tradicionais, com um enfâse reativo, baseavam-se na resposta à ocorrência de crimes, sustentados numa filosofia de controlo e repressão (Oliveira, 2006). Contudo, as transformações sociais contemporâneas,

caracterizadas pela mobilidade transnacional e pelo crime organizado, exigiram a modernização dos modelos de atuação policial.

Diversos modelos foram concebidos para fazer face a esses desafios: o Policiamento Reativo, o Policiamento Preventivo, o Policiamento Orientado pelas Informações, o Policiamento Orientado para a Resolução dos Problemas, entre outros (Rodrigues, 2019). Cada um destes modelos enfatiza diferentes dimensões da intervenção policial: reatividade, prevenção, inteligência criminal, proximidade à comunidade ou eficiência tecnológica.

O modelo de Policiamento Reativo permanece enraizado em ações que respondem à ocorrência de crimes, sendo associado a uma lógica de "combate ao crime" e a uma prática fortemente hierarquizada e militarizada (Rodrigues, 2019). Já o Policiamento Preventivo (, embora de difícil definição operacional, centra-se em medidas proativas para evitar a ocorrência de incidentes, exigindo maior descentralização e envolvimento comunitário (Rodrigues, 2019).

O surgimento do Policiamento Orientado pelas Informações representou uma evolução significativa, pois prioriza a análise e utilização sistemática de dados para a formulação de estratégias eficazes de prevenção e intervenção (Ratcliffe, 2016). Este modelo utiliza ferramentas tecnológicas como Sistemas de Informação Geográfica, reconhecimento facial e vigilância eletrónica para identificar padrões criminais e planear a ação policial. Paralelamente, o Policiamento Orientado para a Resolução dos Problemas centra-se na análise profunda das causas dos problemas de segurança, propondo soluções sustentáveis através da atuação integrada com a comunidade e outros parceiros sociais (Goldstein & Winners, 2001).

Mais recentemente, surgem modelos como o Policiamento de Proximidade e o Policiamento Comunitário, que pretendem aproximar a polícia das comunidades, favorecendo segurança através da participação da comunidade (Kappeler, 2015). O Policiamento Comunitário, em particular, representa não apenas uma técnica, mas uma filosofia organizacional que preconiza a descentralização da tomada de decisão e o reforço do papel das comunidades.

Dentro desta evolução surgem ainda outros modelos como o de Ocupação do Terreno, Concentração de Meios, Dissuasão e Segurança *Just-in-Time*, refletindo diferentes formas de mobilização de recursos e de resposta à criminalidade (Torres, 2015).

É relevante reconhecer que os avanços tecnológicos e a gestão baseada em informações configuram uma polícia mais científica, capaz de atuar tanto de forma preventiva como reativa. No entanto, estes modelos também trazem implicações éticas

relevantes, como riscos para os direitos fundamentais, motivo pelo qual a transparência e a responsabilidade institucional são exigências constantes (Babuta, 2017).

Assim, à luz da dinâmica contemporânea, a evolução dos modelos de policiamento deve articular a busca da eficácia na segurança com a manutenção dos princípios democráticos, em especial no contexto das novas ameaças à segurança pública globais.

1.1. Distinção de *Data Led Policing, Intelligence Led Policing*, Policiamento Preditivo e Policiamento Algorítmico

A utilização de informações e tecnologias pelas FS por todo o mundo tem sido conceptualizada como "policiamento preditivo" (PP), "*Intelligence led policing*" (ILP) e "policiamento algorítmico" (PA). Cada um destes conceitos descreve aspetos importantes da utilização de dados pelas FS: o PP destaca sua capacidade de previsão e prevenção (Van Brakel, 2016); o ILP relaciona o aumento do interesse em táticas de vigilância à evolução de práticas mais tradicionais para atividades mais ligadas à informação (Brayne, 2017); e o PA enfatiza a dependência da tecnologia para interpretar os dados para fins policiais (Egbert, 2019). O que estes conceitos têm em comum é que eles destacam a emergência dos sistemas de dados como uma nova característica do policiamento e enfatizam o impacto na perceção de práticas criminais pelas FS.

O *Intelligence led policing* surgiu no Reino Unido, idealizado por Kent Constabulary, como forma a responder a um aumento de crimes relacionados com o património, numa época em que a os fundos monetários da polícia local estavam a ser reduzidos. Originalmente denominada de *Kent Policing Model*, pretendia priorizar os crimes de maior relevância, disponibilizando mais tempo e recursos para criar equipas de *intelligence,* focadas em criar conhecimento em nove áreas específicas de conhecimento. Após três anos, foi possível diminuir a criminalidade em 24% (Marilyn Peterson, 2005).

O ILP, segundo a *Organization for Security and Co-operation in Europe*, "centra-se na recolha e avaliação sistemáticas de dados e informações, através de um processo de análise definido, transformando-os em produtos de análise estratégica e operacional que servem de base a uma tomada de decisões melhorada, informada e baseada em provas" (2017, p. 8).

Embora seja complicado definir ILP (Khalfa & Hardyns, 2023, p. 3), a definição mais completa para este estudo, concebida por Ratcliffe, dita que o ILP "privilegia a análise e as informações como elementos essenciais de um quadro de tomada de decisões objetivo que

dá prioridade aos pontos críticos de criminalidade, às vítimas repetidas, aos delinquentes prolíficos e aos grupos criminosos. Facilita a redução, a interrupção e a prevenção da criminalidade e dos danos através de uma gestão estratégica e tática, da implantação e da aplicação da lei" (2016, p. 5).

A acrescer, por forma a simplificar a dinâmica do ILP, Khalfa & Hardyns, vêm distinguir três conceitos e três mecanismos de conexão destes conceitos através dos modelos dos três i´s. Os Autores explanam que existe uma relação triangular entre o ambiente criminal, análise de informações criminais e o decisor. Os mesmos referem que a análise de informações criminais, traduz-se num "processo intermédio em que os dados brutos são analisados para os traduzir em "informação", acrescentando-lhes significado ou contexto" (Khalfa & Hardyns, 2023, p. 3), vem interpretar o ambiente criminal e influenciar o decisor, que por sua vez vai criar um impacto, positivo ou negativo no ambiente criminal.

Assim, o decisor afeta o ambiente criminal "desenvolvendo e empregando táticas específicas baseadas em informações criminais derivadas da análise de informações criminais" (Khalfa & Hardyns, 2023, p. 3)

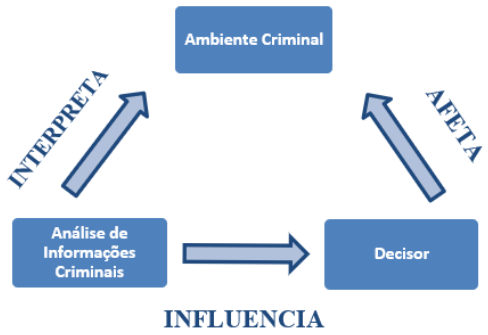

Ilustração n.º 1 – Modelo dos Três I
Fonte: Khalfa, R., & Hardyns, W. (2023). 'Led by intelligence': A scoping review on the experimental evaluation of intelligence-led policing. Evaluation Review.

O PP, não reúne um consenso no que concerne a sua definição, no entanto existem alguns aspetos-chave que são consensuais entre os demais autores que abordam esta temática (Meijer & Wessels, 2019). Embora haja definições focadas para o local, tempo ou na identificação dos indivíduos visados pelas FS, a definição que julgamos mais pertinente fora descrita por Meijer & Wessels e dita que "policiamento preditivo é a recolha e análise de dados sobre crimes anteriores para identificação e previsão estatística de indivíduos ou áreas geoespaciais com uma probabilidade acrescida de atividade criminosa para ajudar a

desenvolver estratégias e táticas de intervenção e estratégias e táticas de prevenção" (2019, p. 1033), o que engloba a questão temporal, que se aplica a um futuro próximo, a questão espacial, a questão de identificação de indivíduos, e ainda mais dois fatores também realçados por os mesmos autores; O uso de dados, não se restringindo a dados criminais, e a vertente da proatividade no âmbito da prevenção criminal (Meijer & Wessels, 2019).

O PA, usa algoritmos[1] para prevenir a criminalidade através de uma análise de dados, incorporando técnicas relacionadas com IA e *machine learning*[2] (Lum & Isaac, 2016). Miró-Llinares dita ainda que o PA se operacionaliza através de "algoritmos para estimar riscos futuros associados a características criminais pessoais ou ambientais, de forma a melhorar a tomada de decisão para fins de prevenção, investigação e persecução do delito" (2020, p. 4).

Sendo estes sistemas fornecidos por empresas privadas, apresentam uma vulnerabilidade relativamente à segurança e confidencialidade dos dados (Lum & Isaac, 2016). O DLP e o ILP constituem-se como duas abordagens distintas, mas interligadas, sobre como as FS utilizam informações para a prevenção criminal.

Ambas representam um avanço significativo na utilização de dados no policiamento contemporâneo, evidenciando a importância crescente da análise de informações. Contudo, apesar das suas semelhanças, estas abordagens diferem em relação à natureza dos dados que priorizam, aos métodos analíticos empregados e aos objetivos estratégicos que as fundamentam.

Enquanto o DLP é definido por uma abordagem abrangente e quantitativa na recolha e uso de dados (Jansen, 2022), o ILP foca-se na análise qualitativa e detalhada de dados criminais específicos, utilizando informações obtidas de maneira mais direcionada e tradicional (Brayne, 2017). Este processo é sustentado por um ciclo de inteligência bem definido, onde a recolha e avaliação de dados tem como objetivo influenciar o decisor, abordando este, por sua vez, áreas de maior relevância criminal, como locais de crime frequente, vítimas habituais e criminosos recorrentes (Ratcliffe, 2016).

No que concerne às similitudes, tanto o DLP quanto o ILP visam otimizar a

[1] Entendidos como um conjunto de instruções com o objetivo de resolver um determinado problema. O seu valor é relativo, sendo determinado pela sua utilidade. Por exemplo, pode ser usado para ordenar alfabeticamente uma lista ou podem ser usados para usar padrões e tendências numa grande base de dados (Lum & Isaac, 2016).

[2] O recurso a técnicas de *machine learning* é importante pois estas têm a capacidade de transformar os *inputs*, dados, em experiência, para obter ter um resultado processado, rico em conhecimento, com uma capacidade de aplicação alta (Shalev-Shwartz & Ben-David, 2014).

distribuição de recursos das FS, o que aumenta a eficácia das respostas ao crime e promove uma abordagem mais informada. Ambas as abordagens empregam dados e análises para fundamentar as decisões, indo além da resposta reativa e focando-se na prevenção da criminalidade através de estratégias proativas. Os dois modelos ressaltam a importância da colaboração entre diversas partes interessadas, utilizando tecnologia e análise para melhorar as operações policiais e aumentar a segurança pública.

Não obstante das similitudes, as diferenças entre as abordagens são substanciais. O DLP baseia-se numa visão integrada que combina grandes volumes de dados, utilizando tecnologias de IA para processar informações. A sua orientação é predominantemente futurista e preditiva, utilizando *Big Data* para prever possíveis focos de criminalidade e para gerir intervenções preventivas em tempo real, enquanto o ILP é mais analítico e focado, com um ênfase claro na conversão de dados específicos em conhecimento estratégico. O ILP prioriza a análise detalhada de dados operacionais de fontes tradicionais, como informações policiais e relatórios de inteligência, aplicando métodos estabelecidos de avaliação e ponderação de ameaças para influenciar decisões a curto e médio prazo.

Segundo Purves et al. (2022) os sistemas de previsão têm sido criticados pela sua opacidade, já que nem os decisores humanos nem os indivíduos afetados conseguem compreender facilmente como as diferentes variáveis influenciam o resultado das previsões. A anonimização e o consentimento informado são fundamentais para uma implementação responsável, algo que não se destaca tanto no ILP, que embora dependa menos de tecnologias avançadas, também enfrenta alguns desafios no que concerne à complexidade de garantir que as decisões sejam fundamentadas em informações precisas e atualizadas.

O conceito de DLP abrange assim a utilização de *Big Data* e o "processo de transformar características da realidade e comportamento social em dados quantificados" (Fontes et al., 2022, p. 2) para expandir as capacidades de vigilância, através de sistemas automatizados que geram e recolhem informações de forma contínua e abrangente. O DLP implica a observação de indivíduos, ou grupos de indivíduos, com a finalidade de fazer inferências sobre os seus comportamentos, podendo ser realizada de maneira retroativa, em tempo real ou proativa, de forma explícita ou oculta (Fontes et al., 2022).

De forma a sintetizar a informação deste capítulo, encontra-se uma tabela com os conceitos chave do DLP, ILP, PP e PA.

	Data Led Policing	Intelligence Led Policing	Policiamento Preditivo	Policiamento Algorítmico
Objeto e Abordagem	Envolvimento abrangente e quantitativo na recolha de dados; usa dados de múltiplas fontes para vigilância contínua e preditiva	Abordagem qualitativa, detalhada, focada na conversão de dados específicos em conhecimento estratégico	Recolha de dados sobre criminalidade anterior para identificar e prever estatisticamente variáveis e probabilidades	Uso de algoritmos para estimar riscos futuros, apoiado em IA e *machine leraning*
Tipo de Dados Utilizados	Big Data, processados por sistemas automatizados, frequentemente envolvendo IA	Informações criminais detalhadas de fontes tradicionais, como relatórios de inteligência e dados policiais	Dados históricos criminais combinados com variáveis contextuais e ambientais	Dados criminais, socioeconómicos e ambientais
Outputs	Orientação proativa e preditiva; antecipação de ameaças em tempo real	Orientado para decisões de curto e médio prazo, mais reativa	Previsões estatísticas sobre locais ou indivíduos com maior probabilidade de cometer ilícitos criminais	Análises de dados e recomendações automatizadas baseadas em IA
Tecnologia	Algoritmos avançados, análise de Big Data, IA, e vigilância automatizada em tempo real	Métodos analíticos tradicionais; depende menos de tecnologias emergentes, mas ainda usa sistemas de avaliação estratégica	Depende de técnicas estatísticas aplicadas a bases de dados criminais	Depende de algoritmos baseados em IA criados por técnicos e *machine learning*,
Ética e Privacidade	Desafios significativos quanto à privacidade, devido à natureza intrusiva e ao uso extenso de dados pessoais	Enfrenta desafios relacionados com a precisão e atualização das informações, mas com menor incisão em questões de privacidade	Apresenta risco de discriminação na análise estatística podendo reforçar desigualdades sociais	Vulnerabilidade na segurança dos dados devido à dependência de fornecedores privados e riscos de enviesamento algorítmico
Colaboração e Parcerias	Envolve parcerias com setores públicos e privados para a recolha de dados em larga escala	Ênfase na cooperação com comunidades locais e outras FSS para recolha de informações	Necessidade de integração com bases de dados governamentais	Forte dependência de empresas externas privadas e especialistas em tecnologias e informações
Impacto Estratégico	Eficiência no uso de recursos e intervenções proativas para gerir a segurança pública	Influencia decisões operacionais e estratégias para abordar crimes frequentes e prolíficos	Permite otimizar a distribuição de recursos e conhecer tendências criminais	Automatiza a tomada de decisões, influenciando as estratégias de policiamento

Tabela 1: Conceitos Chave de DLP, ILP, PP e PA.

Fonte: Elaboração Própria

CAPÍTULO 2 – *DATA LED POLICING*

2.1. Big Data

Para compreender o DLP é vital compreender que dados se tratam quando se fala neste tópico. Entende-se por *Big Data* o conjunto de dados que são recolhidos, analisados, convertidos em algoritmos, num volume infinito, categorizados numericamente e identificados para, posteriormente, extrair informação que capacite e oriente as políticas criminais (Gonçalves, 2017).

As fontes destes dados podem surgir de várias formas como direcionados, por meio de circuitos de câmaras de vigilância, automatizados por localização geográfica detetada pelo dispositivo móvel e voluntários como a autorização de recolha e tratamento dos dados pessoais pelos indivíduos (Lyon, 2014; Chan & Moses, 2015; Lupton & Michael, 2017).

Segundo Yaseen e Obaid (2020), a bibliografia relativa a *Big Data* revela uma diversidade de definições que se agrupam em quatro grandes categorias: Atributos dos dados, necessidades tecnológicas, limiares operacionais e impacto social e cultural. A primeira destaca os atributos fundamentais dos dados, frequentemente sintetizados nos chamados quatro Vs, volume, velocidade, variedade e, mais recentemente a veracidade, salientando a complexidade e a magnitude dos dados processados. A segunda categoria foca-se nas necessidades tecnológicas, enfatizando a utilização de arquiteturas escaláveis e técnicas avançadas como *machine learning* para armazenamento e análise eficiente de grandes volumes de dados. A terceira linha de definição aborda os limiares operacionais, considerando *Big Data* como conjuntos de dados cuja dimensão e complexidade ultrapassam as capacidades das ferramentas tradicionais de gestão e análise. Por fim, uma quarta perspetiva evidencia o impacto social e cultural do fenómeno, conceptualizando o *big data* como um processo que transforma a forma como a informação é analisada e utilizada para compreender e organizar a sociedade.

Geralmente, a definição de *Big Data* envolve três considerações: o grande volume de dados que agrega; a velocidade com que os dados são processados; a variedade dos dados; o formato e a estrutura (Chan & Moses, 2015; Prainsack, 2019).

Bartlett, Lewis, Reyes-Galindo & Stephens (2018) consideram o *Big Data* como a forma de pesquisa indispensável do século XXI, argumentando que as ciências sociais com dados e computação intensiva é um fenómeno contemporâneo (Halford & Savage, 2017). Relativamente ao panorama internacional, o Concelho Europeu, através do *data act*, que

entrou em vigor a 11 de janeiro de 2024, refere que os *Big Data* vieram moldar o mundo, trazendo novos desafios para a proteção de dados.

Podemos então considerar que os *Big Data* fazem uso dos dados para formular teorias sobre os sujeitos que são observados e vigiados, direta ou indiretamente, concretizando assim uma relação entre os sistemas de vigilância e os indivíduos (Ball, Di Domenico & Nunan, 2016).

No entanto a utilização dos *Big Data* acarretam certas limitações. De acordo com o *Royal United Serviçe Institute* (RUSI) (2017), a imensa quantidade de dados sujeita a uma análise e posterior eliminação de variáveis que se demonstram irrelevantes ou não confiáveis, requer uma interpretação bastante subjetiva. É então fator que consagra uma limitação a estes dados a sua não confiabilidade por provirem de diversas fontes que recolheram dados, possivelmente, de formas questionáveis (Babuta, 2017). Boyd & Crawford afirmam que "(…) os grandes conjuntos de dados provenientes de fontes da Internet são muitas vezes pouco fiáveis, propensos a falhas e perdas, e estes erros e lacunas são ampliados quando são utilizados vários conjuntos de dados em conjunto" (2012, p. 668).

Os elevados requerimentos técnicos também contribuem como um fator limitador, visto que não é só relevante um bom processador, mas também uma boa e segura capacidade de armazenamento. Devido à sensibilidade dos dados, o setor publico no seu panorama geral têm-se mostrado apreensivo em apostar neste armazenamento de dados, especialmente pela suscetibilidade às leis de proteção de dados (Babuta, 2017), o que "é especialmente verdade para a polícia, que lida com grandes volumes de dados pessoais" (Babuta, 2017, p. 18).

Como é referido por Boyd & Crawford (2012), a evolução dos *Big Data* acarreta complexas questões éticas pragmáticas. A par da evolução da tecnologia, também a legislação se vai adaptando, alastrando a novas áreas e progressivamente evoluindo para uma panóplia de "(…) novas regras para regular o custo social das nossas novas ferramentas sem sacrificar os seus inegáveis benefícios" (Richards & King, 2014, p. 409). De forma a mitigar os riscos no que concerne aos trâmites legais, "os requisitos de privacidade e o consentimento informado dos utilizadores afetados são condições preliminares e a anonimização é fundamental para não ultrapassar as normas de privacidade" (Fontes et al., 2022, p. 5)

Atualmente, "a legislação relativa à proteção de dados é altamente complexa e matizada, e os profissionais não dispõem de uma fonte de orientação acessível e prática sobre o que constitui uma utilização adequada dos dados" (Babuta, 2017, p. 49), o que para as FSS constitui uma ambiguidade no que concerne à tomada de decisão nestas matérias. De forma

a ver colmato este desafio de matéria jurídica, *o Science, Innovation and Technology Committee*[3] em colaboração com a Durham Constabulary, criou um sistema de apoio à tomada de decisão nas FS, denominado de *ALGO-CARE*, "(…) que se destina a fornecer orientações para a utilização de ferramentas de avaliação dos riscos, de previsão, de classificação, de tomada de decisões e de assistência ao policiamento que incorporem métodos algorítmicos de aprendizagem automática e que possam ter impacto nos indivíduos a nível micro ou macro" (Oswald & Grace, 2017, p. 2).

Da análise convergente destas abordagens, resulta uma definição que dita que "*Big Data* representa ativos de informação caracterizados por um volume, velocidade e variedade tão elevados que requerem tecnologias e métodos analíticos específicos para a sua transformação em valor" (Yaseen & Obaid, 2020, p. 46). Por abranger todos os conceitos mencionados e ressalvados anteriormente, é a definição que aparenta ser mais completa, concisa e adequada para o propósito da investigação.

Por forma a ressalvar melhor os conceitos relativos a *Big Data*, apresenta-se infra uma tabela com os cinco principais pilares realçados igualmente por Andrade (2022).

Pilares	**BIG DATA**	
Volume	Grande volume de informações, exigindo uma infraestrutura de processamento e armazenamento robusta.	Chan & Moses (2015); Prainsack (2019)
Velocidade	Análise e Processamento em tempo real.	Chan & Moses (2015)
Variedade	Todos os dados quantitativos e qualitativos.	Prainsack (2019)
Veracidade	Variável, exigindo validação e filtragem.	Boyd & Crawford (2012); Babuta (2017)
Valor	Elevado valor, através de *insights* nas demais áreas de aplicação.	Bartlett et al. (2018)

Tabela 2: Conceitos de *Big Data*

Fonte: Elaboração Própria

[3] Comité de Ciência, Inovação e Tecnologia, responsável por examinar os gastos, a administração e as políticas do Departamento de Ciência, Inovação e Tecnologia, bem como de organismos públicos associados. Além disso, assegura que as decisões governamentais em diversos departamentos sejam fundamentadas em evidências científicas sólidas e aconselhamento técnico adequado (UUK, 2025).

2.2. O Data Led Policing

Numa sociedade cada vez mais dependente da Inteligência Artificial[4] (IA) e fazendo uso da sua evolução, é relevante analisar a seu contributo na segurança interna, como é explanada no n.º 1 do Art.º 1º da Lei de Segurança Interna.

Como referido por Kearns & Muir (2019), a transformação do contexto requer, inevitavelmente uma mudança na natureza do policiamento. Pretende-se ressalvar que não se pode combater a criminalidade do presente e do futuro com tecnologias do passado. Exemplo desta evolução é a utilização de diversos dispositivos, denominados *Internet-of-Things* (IoT), como por exemplo os recetores de áudio.

Segundo CBS (2015), a utilização de dispositivos IoT em Camden, New Jersey, permitiu à Polícia Local averiguar que 38% dos disparos num determinado bairro não eram reportados, o que possibilitou posteriormente uma melhor alocação dos recursos.

O DLP vem marcar uma nova era nos dados, que agrega uma multiplicidade de tecnologias em que as FSS estão interessadas (Jansen, 2022). Fontes et al., definem DLP ou *Dataveillance* como "tirar partido dos *Big Data* para aumentar a vigilância" (2022, p. 2) e referem como principais atributos a "recolha e tratamento de dados pessoais incluindo, em tempo real, empregando sistemas automatizados e monitorizadores de rotinas e a identificação, seguimento, regulação, previsão, prescrição, prevenção e orientação de comportamentos de indivíduos ou grupos" (2022, p. 2).

Kearns & Muir interpretam o DLP como "a aquisição, a análise e a utilização de uma grande variedade de fontes de dados digitalizados para informar a tomada de decisões, melhorar os processos e aumentar informações acionáveis para todo o pessoal de um serviço policial, quer estejam a operar na linha da frente ou em posições de liderança estratégica" (2019, p. 2). Os mesmos autores referem que esta evolução, o DLP, traduz-se no aumento do valor público das FS, isto é "(…) o valor total que uma força policial contribui para a sociedade numa série de dimensões mensuráveis, incluindo os resultados em matéria de em relação à criminalidade, a utilização eficaz dos fundos públicos e a qualidade da relação da polícia com o público" (Kearns & Muir, 2019, p. 6).

No cerne do DLP está a análise e a utilização de uma ampla gama de dados, que vão desde registos de incidentes criminais e dados demográficos até informações provenientes

[4] em "(…) termos gerais entendida como um domínio da ciência da computação que procura criar máquinas que imitem a inteligência humana" (Schuetz et al., 2020, p. 2).

de redes sociais e vigilância em tempo real. Esta recolha abrangente e a aplicação de algoritmos não apenas permitem a monitorização e o mapeamento de crimes em tempo real, mas também a previsão e a intervenção em potenciais focos de criminalidade (Kearns & Muir, 2019). A utilização destes dados representa uma nova abordagem, onde as informações recolhidas são sistematicamente integradas e analisadas para gerar outputs. A análise de dados é fundamental para identificar padrões de comportamento e tendências criminais, permitindo que as FSS atuem de maneira mais eficaz e direcionada, evitando intervenções desnecessárias e otimizando os recursos disponíveis (Jansen, 2018; Jansen, 2022).

Fontes et al. (2022) explicam que o eficaz funcionamento do DLP assenta na utilização combinada de dados armazenados e gerados em tempo real, tirando partido da interconexão, da elevada capacidade de processamento e da automatização dos sistemas presentes tanto na esfera pública como na privada. Esta abordagem representa um avanço em vários domínios, nomeadamente na produtividade e eficácia das forças de segurança, incluindo a prevenção criminal.

O conceito de DLP está profundamente relacionado ao uso extensivo de *Big Data*, que envolve dados de múltiplas fontes, tanto públicas quanto privadas, e integra tecnologias avançadas para processamento e análise em tempo real. A abordagem do DLP tem como objetivo criar um ambiente de vigilância contínua, monitorizando atividades criminosas através de sistemas automatizados que analisam grandes quantidades de dados simultaneamente. O DLP concentra-se na identificação de padrões e na previsão de comportamentos futuros, permitindo intervenções proativas antes que os crimes aconteçam. (Kearns & Muir, 2019)

Com base em algoritmos avançados e análises retroativas e preditivas, o DLP apoia políticas de segurança pública que antecipam ameaças em diversos contextos, desde a prevenção de crimes de rua até a mitigação de riscos cibernéticos (Kearns & Muir, 2019).

A combinação dos fatores referidos no âmbito do DLP traduz-se na utilização de dados armazenados e em tempo real, recorrendo à interligação de sistemas, ao processamento rápido de informação e à automatização em contextos públicos e privados. Segundo Fontes et al. (2022), esta abordagem contribui para avanços significativos em diversas áreas, como a produtividade e o bem-estar das forças de segurança, bem como na melhoria da investigação, deteção e prevenção da criminalidade.

Não obstante dos corolários considerados anteriormente, o DLP enfrenta desafios éticos e técnicos consideráveis. A utilização de *Big Data* na segurança do domínio público

levanta questões relacionadas com a questão da privacidade e da proteção de dados, especialmente devido à diversidade e à falta de confiabilidade das fontes, conforme destacado por Boyd e Crawford (2012). A exigência de um rigor técnico e de uma infraestrutura sólida para o processamento e armazenamento de dados, também se considera como um fator que impõe barreiras significativas à sua implementação eficaz. A anonimização dos dados e o consentimento informado dos indivíduos envolvidos são práticas essenciais para garantir que o DLP respeite os direitos civis e opere em conformidade com as normas de proteção de dados, sendo essas questões cruciais para o seu uso ético e responsável no âmbito da segurança pública (Babuta, 2017; Fontes et al., 2022).

O DLP levanta desafios relevantes no que diz respeito à legislação de proteção de dados e às questões éticas associadas à privacidade e ao risco de discriminação, devido ao seu amplo alcance e ao carácter potencialmente intrusivo da monitorização que realiza. De acordo com Saheb (2023), a principal preocupação dos cidadãos prende-se com a proteção dos seus dados pessoais, sobretudo no que toca à forma como são utilizados, ao risco de acessos ilegais e à possibilidade de ciberataques que comprometam os serviços das cidades.

2.3. O Data Led Policing e a Prevenção Criminal

São inúmeros os autores que definem prevenção criminal, no entanto a definição que mais se relaciona com a investigação é descrita por Cusson dita que a "prevenção significa agir de forma proativa e não coercitiva com vista a reduzir a frequência ou a gravidade das infrações" (2007, p.49).

A prevenção distingue-se em três tipos, a prevenção primária, secundária e terciária (Alves, 2008; Sampaio, 2021):

A primária, que se foca nos cidadãos como um todo, analisando todo e qualquer cidadão mesmo que não estejam referenciados ou associados a atividades criminosas, como é evidenciado por Sento-Sé (2011), que dita que a prevenção primária é abrangente e articula a identificação de áreas e grupos que possam estar em risco de serem afetados pela violência, ates que ela se concretize.

A prevenção secundária, que como descrita por Machado da Silva "é destinada a pessoas ou grupos envolvidos em processos de criminalização e tem como objetivo garantir medidas educativas em alternativa a prisão" (2009, p. 120), surgem nos programas especiais de prevenção criminal, orientados para determinados grupos de pessoas, numa determinada zona e expostas a circunstâncias possivelmente danosas.

A prevenção terciária segundo Andresen & Jenion, (2008), visa prevenir a

reincidência criminal de pessoas que já estejam sob o controlo do sistema de justiça penal. Funciona essencialmente através das reabilitações e das ações desenvolvidas no âmbito da proteção e reinserção social dos indivíduos identificados.

Welsh & Farrington (2011) distinguem ainda três estratégias de prevenção criminal. A prevenção comunitária que versa sobre as condições sociais e as instituições que têm influência no abandono das comunidades residenciais; A prevenção situacional que se define por uma abordagem preventiva que tem como principal objetivo a diminuição da oportunidade de cometer crimes e não necessariamente na melhoria da sociedade, como referido igualmente por Clarke (1992). Welsh & Farrington referem-se a esta como "intervenções concebidas para prevenir a ocorrência de crimes, reduzindo as oportunidades e aumentando o risco e a dificuldade de os cometer" (2011, p. 4) e a prevenção pelo desenvolvimento que atua no desenvolvimento do criminoso, abordando fatores de risco e de proteção ao longo do desenvolvimento humano (Welsh & Farrington, 2011).

No que concerne a prevenção criminal, o DLP é enfatizado pela sua abordagem não punitiva, que pretende dissuadir a criminalidade através de uma gestão estratégica de recursos. Deste modo é destacada importância das FSS anteciparem riscos e adotarem uma postura proativa ao invés de responder a delitos (Fontes et al., 2022). O DLP possibilita que as políticas de segurança sejam moldadas não apenas para atuar em áreas com alta incidência criminal, mas também para mitigar ameaças associadas ao crime organizado, terrorismo, uso de armamentos perigosos e crimes de natureza cibernética. São fatores que se tornam cada vez mais relevantes no cenário atual, especialmente com o avanço das tecnologias digitais (Lei de Política Criminal, 2023).

A importância do DLP é ainda mais acentuada pela potencialidade de fortalecer a relação entre as FSS e a comunidade, ampliando o valor público[5] gerado, conforme destacado por Kearns e Muir (2019). Ao fomentar uma segurança do domínio público mais eficiente e fundamentada, o DLP trabalha no domínio da prevenção criminal que tem essencialmente dois objetivos, sendo que "o primeiro é o decréscimo da criminalidade, e o segundo é o aumento do sentimento de segurança por parte dos cidadãos, mantendo entre si uma relação inversa, pois, se a criminalidade diminuir, o sentimento de segurança aumenta

[5] Neste contexto, interpretado como o produto das FS na sociedade, que pode ser avaliado em diversas dimensões, nomeadamente o uso de fundos públicos, a qualidade das relações entre as FS e os demais cidadãos e a sua atuação (Kearns & Muir, 2019).

e vice-versa" (David, 2014, p. 12). Este valor público não se limita à diminuição da criminalidade, mas também se reflete na eficiência do uso de recursos públicos e na capacidade das FSS de se adaptarem a uma realidade social em constante transformação (Kearns & Muir, 2019).

No que concerne a prevenção criminal, relativamente ao DLP, podemos situar a mesma na prevenção situacional, visto que visa identificar áreas propensas à criminalidade, permitindo a adaptação do policiamento noutras intervenções preventivas para minimizar oportunidade de delitos. Este método adotado de prevenção criminal pode ter em conta um determinado grupo demográfico específico ou uma determinada área geográfica com base nas suas tendências. Deste modo o DLP pode ser usado como uma ferramenta de prevenção primária e secundária prevenindo tanto a primeira ocorrência como a sua reincidência.

O DLP configura-se assim como uma abordagem inovadora e abrangente para a prevenção criminal, cuja eficácia reside na sua capacidade de prever e mitigar riscos, não obstante de surgirem algumas reservas no que diz respeito a questões éticas e técnicas da sua implementação e do uso funcional. A relação entre o potencial preventivo do DLP e os desafios da sua aplicação prática evidencia a complexidade e as repercussões desta abordagem para o policiamento atual, dando lugar a uma nova era da segurança pública.

2.4.*Data Led Policing* na República Popular da China

Na RPC, assim como no resto do mundo, prevenção criminal está associada à dissuasão, evitando que infratores cometam crimes no futuro. Os recentes avanços na digitalização e automatização na prevenção criminal refletem a tendência crescente do investimento na segurança pública na RPC (Spick, 2019), nas políticas de prevenção criminal e no uso generalizado de tecnologia de vigilância (Ji, 2021). A última atualização do Código Penal da RPC, *Criminal Law of People´s Republic of China*, vem reforçar a ideia de punição aliada ao conceito de prevenção (Ji, 2021). Ji (2021) refere que, no contexto da RPC, a prevenção relaciona-se com a imposição de penalizações criminais, sem que tenha sido causado um dano real. Para além dos crimes previstos no capítulo segundo, secção dois denominado de preparação de um crime, tentativa criminal e interrupção de um crime. Para além dos crimes aqui previstos, esta atualização vem criminalizar a condução sob efeito de álcool, produção e venda de medicamentos falsificados e poluição ambiental. A criminalização destas práticas vem controlar o risco de novas ocorrências para evitar danos no futuro.

Para além de se justificar com o próprio Direito Penal, a prevenção surge também

como uma justificação para o Processo Penal, o que na visão da RPC, implica necessariamente um policiamento mais intensivo e uma *surveillance* mais alargada (Jin, 2021). A importância deste tema para o Estado é relevada pelas declarações de Xi Jinping numa conferencia de segurança em que faz a seguinte declaração:

Temos de aumentar a socialização, o nível do Estado de direito, a inteligência e o profissionalismo da nossa governação social e aumentar a capacidade de prever, alertar e prevenir qualquer tipo de risco. [...] Aperfeiçoaremos os nossos mecanismos de *governance* social para a segurança pública e trabalharemos rapidamente na integração e informatização do sistema de prevenção e controlo da nossa segurança pública (Xi Jinping, 2016)

Ainda é notável uma flexibilidade no poder e na autoridade da polícia e do Estado, que continua com autonomia para vigiar e investigar crimes contra o mesmo e contra a ordem social. Segundo Ji (2021) o crime é usado como desculpa para legitimar determinadas ações por parte do Estado, como por exemplo a restrição da liberdade de associação, com o pretexto da proteção de uma harmoniosa ordem social ou a monotorização de discursos e atividades públicas que podem atentar à segurança do Estado.

Relativamente à proteção de dados pessoais, ainda que exista uma lei que a assegure, a Lei de Proteção de Informações Pessoais da RPC (LPIP), que dita que o processamento de informações pessoais se deve basear essencialmente nas mesmas bases legais do Regulamento Geral de Proteção de Dados (RGPD), excetuando-se o reconhecimento de interesses legítimos do interessado (LPIP, 2022), esta é facilmente contornada pela Lei de Segurança do Estado (LSE), que dita que qualquer órgão de segurança pública e militares em cargos de relevo podem recolher informações relativas à segurança nacional (LSE, Art.º 52º). Esta indiscrição viola os demais direitos internacionais referentes a estas matérias, mesmo sendo legítimo, pois não refere a proporcionalidade e a necessidade da recolha e processamento dessas informações (HRW, 2019).

Com uma total de 1,412,360,000 de pessoas, aproximadamente, segundo o *Global Organized Crime Index (2023)*, é vital possuir um sistema de segurança bastante evoluído. Estima-se que a RPC possua o maior sistema de vigilância em massa do mundo, com aproximadamente 540 milhões de câmaras de vigilância instaladas em todo o território, o que equivale a quase uma câmara para cada duas pessoas (Creemers, 2018).

Este conjunto de desenvolvimentos contribui para a construção de sociedades organizadas em *Smart Cities* (SC). Do ponto de vista académico, estas têm sido descritas como estruturas complexas e pouco coesas, marcadas por ambiguidade, fragmentação e falta de clareza na sua definição (Hu, 2019). Harrison et al. (2010) propõem uma definição

centrada em três pilares fundamentais: a instrumentalização, que corresponde à recolha e integração em rede de dados provenientes de sensores, dispositivos pessoais e outros equipamentos de IoT; a interconectividade, que consiste na capacidade de integrar essa informação em plataformas que garantem a comunicação e interoperabilidade entre serviços; e a componente de inteligência, entendida como a aplicação de análises complexas, modelação e otimização de dados para apoiar decisões ao nível operacional.

Marsal-Llacuna et al. (2014) afirmam que as SC procuram melhorar o desempenho urbano, utilizando *Big Data* e demais Tecnologias de Informação e Comunicação (TIC). Desta forma, as SC permitem a prestação de serviços sociais mais eficientes à população, a monotorização e otimização de infraestruturas pré-existentes e um aumento na colaboração entre agentes económicos, públicos e privados, demonstrando que uma SC é compreendia como tendo uma capacidade intelectual que integra aspetos sociotécnicos e socioeconómicos que proporcionam o crescimento da sociedade (Zygiaris, 2013).

Na RPC, segundo Zhu et al. (2024), as SC podem ser divididas e organizadas em cinco categorias. As SC são ordenadas segundo o objetivo seja este os recursos humanos ou as estruturas e IoT associadas ao funcionamento da SC, a participação da população e o *output* ou o resultado de todo o processo, como por exemplo "mobilidade, segurança, saúde e *governance* inteligente" (Zhu et al., 2024, p. 7). Na tabela seguinte estão, de forma sumária, apresentados os tipos de SC.

Tipo de SC	**Características**	**Principais SC**
SC Tecnocráticas e baseadas no conhecimento	Ênfase nos recursos humanos, no espírito empresarial e nas infraestruturas de TIC, participação passiva dos cidadãos, resultados monodimensionais.	Xinyu, Liaoyuan, Shenyang, Guigang, Jining, Pingxiang, Rushan, Suqian, Wanning, Weihai, …
SC Holísticas	Ênfase nos recursos humanos, no espírito empresarial e nas infraestruturas de TIC, com um certo grau de participação dos cidadãos, resultados pluridimensionais.	Beijing, Zhuhai
SC "Verdes"	Ênfase nos recursos humanos, no empreendedorismo e nas infraestruturas de TIC, participação passiva dos cidadãos, resultados multidimensionais com ênfase no desenvolvimento ecológico e com baixas emissões de carbono.	Shenzhen, Bozhou, Changzhou, Chengdu, Fuzhou, Fuyang, …
SC Tecnocráticas	Ênfase na infraestrutura de TIC, orientada para a	Yantai, Qinzhou, Jinan

apoiadas em IoT	tecnologia com participação passiva dos cidadãos, resultados monodimensionais.	
SC Emergentes	Contribuição limitada em termos de recursos humanos, espírito empresarial e infraestruturas de TIC, participação passiva dos cidadãos, resultados monodimensionais.	Ningguo, Changji, Huanggang, Luoyang, Siping, Xinzheng, Xianning, Zhengzhou.

Tabela n.º 3: Tipos de SC na RPC e descrição sumária

Fonte: Zhu et al. (2024). How different can smart cities be? A typology of smart cities in China. Cities.

Na imagem seguinte está explanado de forma perfeita o funcionamento de uma SC, neste caso a de Shenzhen, que é um uma SC que se desenvolveu mais e mais rápido que qualquer outra, nomeadamente Pequim, Shanghai ou Hangzhou (Große-Bley & Kostka, 2021). Shenzhen deve ser analisada de perto por diferentes fatores, primeiramente por ter passado de projetos piloto para uma SC em menos de dez anos e por ser cidade natal de empresas de tecnologia com presença mundial como a *Tencent* e *Huawei*. O Partido realçou o destaque e a evolução de Shenzhen ao apontar esta mesma SC para um projeto de região *Smart*, e tornando-a de modelo para as restantes SC (Große-Bley & Kostka, 2021).

Na camada base, mais primária, apresenta-se a rede sensores, responsável pela recolha de dados em tempo real através de sensores, redes associadas e instrumentos IoT como sensores de tráfego, sensores ambientais, sensores de vídeo e os sensores de redes socais que capturam dados de tendências e comportamentos. Segundo Hu (2019) a "instalação de sensores e câmaras em toda a cidade, especialmente nos espaços públicos, coloca toda a cidade sob monitorização e vigilância". Ainda se insere nesta camada as redes de *governance*, que liga dados e serviços governamentais. Para processar e armazenar estes dados, nesta camada, apresentam-se os *Data Center* (DC*)* municipais e distritais.

Analisando a camada intermédia, observamos que é composta por um DC urbano de *Big Data* e por um Centro de Operações e Gestão da SC, onde ocorre o processamento e gestão dos dados recolhidos pela primeira camada. O DC urbano armazena e centraliza os dados numa plataforma denominada de Plataforma de Recursos de Dados, através de uma análise dos grandes volumes de dados extai *insights*. Este DC promove a partilha e troca de dados entre os sistemas e diversos setores, através da IA que interpreta os dados e permite uma apresentação clara das informações. O Centro de Operações e Gestão da SC suporta

todo este processo através de uma *cloud*[6] que gere recursos e facilita a interação entre empresas e governo.

A camada superior é composta por quatro vertentes, serviços públicos, segurança publica, *governance* urbana e indústria *smart*. Estas vertentes representam a aplicação prática das análises nas camadas inferiores, tendo agora impacto direto na vida dos cidadãos. O objetivo desta camada é utilizar os dados para aprimorar serviços, a segurança e otimizar o governo e o desenvolvimento económico.

Todo este sistema é apoiado por dois pilares fundamentais: Apoio à Normalização e Regulação e Apoio à Rede e à Segurança[7]. Estes estabelecem as diretrizes para o funcionamento do sistema e garantem a proteção dos dados e a conectividade entre os elementos desta cadeia.

De forma sucinta, os dados são recolhidos na primeira camada sensorial, processados e analisados na segunda camada e utilizados para apoio na tomada de decisão e melhoria dos serviços públicos na terceira camada. É deste modo que as SC se organizam variando na instrumentalização da primeira camada, recebendo outro tipo de *inputs* para o sistema, havendo outro tipo de análise e processamento conforme o resultado prático que se pretende e na terceira camada, pois quando o *input* é diferente o *output* será naturalmente diferente e com aplicações distintas.

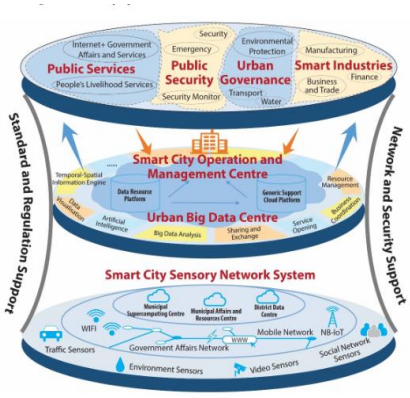

Ilustração n.º 2 – Funcionamento de uma SC

Fonte: Hu, R. (2019). The State of Smart Cities in China: The Case of Shenzhen. *Energies*, *12*(22), 4375. https://doi.org/10.3390/en12224375

[6] Os sistemas de *Cloud Computing* oferecem a capacidade de armazenar dados de forma segura e confiável, podendo ser acedidos em qualquer momento em qualquer lugar, em servidores compartilhados e interligados pela internet, sem perigo de perda de informação, vírus ou outros constrangimentos (Pinheiro, 2014).

[7] [7]*Standard and Regulation Support* e *Network and Security Support.*

Analisando a RPC, e situando-a no panorama internacional, segundo o *Safety Perceptions Index 2023*, apresenta-se em nono lugar no que concerne à perceção dos cidadãos em diversas matérias, avaliando as suas preocupações e experiências recentes.

Relativamente à Ordem e Segurança, exclusivamente, a RPC encontra-se na 40ª posição do ranking da *World Justice Project – Rule of Law Index 2024*, de 142 países, na vertente de segurança e ordem pública, no entanto encontra-se na 139ª posição na variável que avalia a proteção dos demais direitos fundamentais dos cidadãos.

Desde a sua criação, em 1949, a preservação da estabilidade social tem sido considerada vital para assegurar o controlo do poder. Uma característica distintiva da abordagem chinesa em relação à segurança interna [8]é a vasta infraestrutura de vigilância pública e a repressão de dissidentes e movimentos que possam ameaçar a ordem social (Liang & Chen, 2022).

Esta abordagem é possível devido à natureza autoritária e de poder centralizado do regime em causa através de uma guerra de informações e de operações de influência, *information warfare and influence operations* (IWIO), que têm cada vez mais ganho relevância pela evolução da IA (Hunter et al., 2024). É no intuito desta IWIO que se procede a uma recolha de *data* extensiva através de métodos mais invasivos, vigiando a sua população, não tendo como preocupação a sua privacidade ou demais liberdades civis, que posteriormente se utiliza para aprimorar algoritmos utilizados nessa mesa IWIO (Hunter et al., 2024).

Por detrás dos objetivos do PCC e desta IWIO, que passam essencialmente por "controlar a população doméstica disseminar as narrativas políticas" (Hunter et al., 2024, p. 242) do regime, apresenta-se a plataforma *WeChat*[9], que surge como uma plataforma social que recolhe *data* no sentido de trabalhar para os interesses do regime na IWIO. (Hunter et al., 2024).

Como explanado por Hunter et al. (2024), a IWIO, apesar de aqui se considerar o termo "guerra" não se exclui o seu uso noutro contexto. Também num espaço definido como

[8] A segurança interna, na visão da RPC, está explanada no Art.º 2º da Lei Criminal da RPC e entende-se pela soberania da ditadura democrática do Partido e do sistema socialista, pela proteção das propriedades do Estado, dos trabalhadores e demais cidadãos, dos direitos dos cidadãos, manutenção da ordem pública e económica, e por último, pelo garante de uma progressão socialista.

[9] A principal aplicação de *social media* da RPC, desenvolvida pela empresa *Tencent* situada em Shengzhen, é usada para uma multiplicidade de aplicações desde comunicação a pagamentos, sendo que se estima que 60% das transferências monetárias da RPC são através desta aplicação (Hunter et al., 2024, p. 242).

zona cinzenta, entre a paz e a guerra, como referido por Tiwari (2022), a RPC utiliza a IWIO para disseminar propaganda, incorporar uma vertente psicológica nas operações e controlar o espaço digital, através da desinformação com o intuito de desmoralizar os inimigos e aumentar a polarização nas democracias ocidentais (Hunter et al., 2024).

A importância do espaço ciber, informações e em todo o espectro eletromagnético é realçada pela disrupção de uma força por meio de fracos resultados, que fora constituída em 2015 com o objetivo de ganhar vantagem estratégica nesses campos sendo que atualmente são dois departamentos designados de *Aerospace Force* e *Cyberspace Force* que ficaram encarregues dessas atribuições (Hunter et al., 2024). Denotamos assim um acrescido reconhecimento da IA como um fator que proporciona o crescimento, a perturbação e o controlo no espaço das informações, mas também na monotorização e controlo da população (Hunter et al., 2024).

2.4.1. Instrumentalização do DLP

2.4.1.1. Sistema de Crédito Social na RPC

Atualmente, vigora uma abordagem inovadora, que utiliza a IA para quantificar e qualificar o comportamento dos cidadãos, denominado de Sistema de Crédito Social (SCS). Através de algoritmos complexos, a informação, denominada *data,* obtida de câmaras de vigilância, registos financeiros e interações sociais, gera pontuações que refletem a confiabilidade e moralidade de cada indivíduo (Liang & Chen, 2022).

Este sistema que aparenta ser meramente um utensílio de análise de carácter, também se configura como uma ferramenta emergente para reforçar o controlo social, impondo sanções àqueles que infringem normas ou exibem comportamentos antissociais e premiando aqueles que se demonstrem merecedores de tal destaque, quer seja no campo do mérito quer seja no ramo empresarial (Kostka, 2019). Por exemplo, "os cidadãos elegíveis podem beneficiar, por exemplo, de descontos no estacionamento, nos transportes públicos e ginásios públicos. Podem também obter dispensa de caução em bibliotecas e hospitais, *fast-tracks* em escolas, hospitais e outros serviços públicos" ao passo que cidadãos mal classificados "não podem obter prémios e prémios e louvores dos governos locais e são proibidos de trabalhar nos governos e instituições públicas" (Liang & Chen, 2022, p.13).

Surge assim uma aplicação do DLP numa sociedade funcional. Os *Big Data*, surgem como a grande fonte de informação para desenvolver análises capazes de definir parâmetros de comportamentos e surge como um meio para organizar e corrigir os dados, verificar as

fontes e ajustar os algoritmos (Backer, 2019) para o objetivo pretendido: criar uma sociedade construída em torno de uma noção de bondade, credibilidade e confiança, à medida do PCC, pela identificação de todos cidadãos (Creemers, 2018), criação de perfis desviantes e moldando o comportamento individual (Liang & Chen, 2022).

O SCS, através do poder conferido pelo PCC, e pelas implicações que o tornam eficaz, reprime qualquer dissidência com o uso da força ou por instrumentalização de IoT, sufoca a sociedade civil independente de salvaguardar os seus interesses, e de várias perspetivas torna o Estado imoral (Dubois de Prisque, 2020).

A instrumentalização da IoT refere-se à capacidade de recolher, monitorizar e integrar, em tempo real, grandes volumes de dados provenientes de uma vasta rede de sensores, dispositivos pessoais, sistemas urbanos e infraestruturas inteligentes (Harrison et al., 2010). No domínio da segurança pública, esta instrumentalização manifesta-se, por exemplo, na implementação de câmaras de videovigilância dotadas de reconhecimento facial, sensores acústicos para deteção de disparos, leitores automáticos de matrículas, bem como na utilização de dispositivos móveis utilizados pelas FS no terreno com acesso direto a bases de dados das mesmas FS. Um exemplo notável é o sistema *ShotSpotter*, implementado em várias cidades dos Estados Unidos, que utiliza microfones distribuídos estrategicamente em áreas urbanas para identificar a origem de disparos e notificar em segundos as autoridades competentes (Piza, 2024). Outro caso relevante é o da cidade de Barcelona, onde sensores de movimento e câmaras ligadas a sistemas de inteligência artificial monitorizam comportamentos suspeitos em tempo real em zonas críticas (Hu, 2019). Estes dispositivos permitem gerar dados contínuos e georreferenciados, essenciais para alimentar algoritmos preditivos usados no DLP. A instrumentalização de IoT favorece a interoperabilidade entre diferentes serviços urbanos, permitindo respostas articuladas entre FS, proteção civil e serviços de saúde. Este tipo de integração encontra-se, por exemplo, em sistemas como o *City Brain*, desenvolvido na cidade de Hangzhou, onde câmaras, semáforos e sensores ambientais estão ligados a uma plataforma central que gere automaticamente o trânsito, alerta para emergências e sugere rotas para viaturas das FS e ambulâncias (Caprotti, F., & Liu, D. 2022).

2.4.1.2. Golden Shield Project

O *Golden Shield Project* (*GSP*) foi uma iniciativa do governo da RPC nos anos 2000 que tinha como objetivo obter controlo social e aumentar o combate à criminalidade, através

de uma vasta infraestrutura de controlo e vigilância (Wang, 2019).

O GSP, desde os Jogos Olímpicos de 2008 em Pequim, sob o pretexto de manutenção da estabilidade, tem vindo a ser expandido, atribuindo-se recursos "às agências de segurança para monitorizarem dissidentes, desmantelarem protestos, controlarem a Internet e desenvolverem e implementarem sistemas de vigilância em massa" (Wang, 2019, pp. 11 e 12). Segundo Wang (2019), a atribuição de um cartão de identificação, a gigante rede de câmaras de vigilância e as tecnologias de IA permitem ao PCC identificar pessoas instantaneamente, sendo que este circuito é realizado sem qualquer tipo de respeito ou consideração pelos direitos dos cidadãos em prol da segurança do Estado.

Analisando o caso de Xinjiang, uma região autónoma da RPC, surge uma plataforma denominada *Integrated Joint Operations Plataform* (IJOP). Perante a ameaça do separatismo, terrorismo e extremismo, a IJOP tem recolhido *data* de uma variedade de formas, como por exemplo *wifi sniffers*[10], amostras de material genético, scans da iris e amostras de sangue de todos os cidadãos dos 12 aos 65 anos. Ainda se acrescenta a esta lista uma gravação de voz requerida a todos os cidadãos que pretendam um passaporte (Wang, 2019).

Toda esta informação está centrada numa base de dados acessível pela polícia e está anexada ao número de identificação de cada pessoa. Existem ainda mais um projeto que o PCC usa para obter mais *data*: a *Fanghuiju*[11], que possibilita a realização de visitas domiciliárias intrusivas, durante as quais funcionários públicos recolhem dados adicionais diretamente nas residências dos cidadãos. As ferramentas exemplificam a forma como a vigilância digital é operacionalizada através de mecanismos tecnológicos integrados, reforçando o controlo social de forma contínua e sistemática (Wang, 2019).

O IJOP, tem como principais objetivos a recolha de *data*, o preenchimento de relatórios sobre pessoas, veículos, objetos ou eventos suspeitos, e a realização de missões de investigação, e para tal recorre a um algoritmo para identificar 36 tipos de pessoas que requerem especial atenção. Estas categorias diferem em função do *data* recolhido de

[10] Os avanços tecnológicos e na consequente evolução do *wifi*, permitiram criar uma infraestrutura denominada *wifi sniffer*. Esta é capaz de extrair informação como localização, movimentos e outras atividades analisando a conectividade entre o dispositivo e os pontos de acesso(Li et al., 2020).

[11] Fanghuiju é uma abreviação da expressão visitar o povo, beneficiar o povo e reunir os corações do povo e consiste num projeto que prevê visitas domiciliárias regulares para recolha de dados pessoais e familiares; a promoção de educação ideológica e legal orientada para reforçar o sentimento de pertença à nação chinesa; o apoio social e económico a famílias vulneráveis; e o fortalecimento da presença do PCC nas comunidades, através da reorganização dos comités locais e do recrutamento de novos membros (Bao, 2020).

determinada pessoa. Essas informações vão desde material genético a *status* religioso e político, e permitem identificar pessoas não oficialmente imã até pessoas que não socializam com os vizinhos, demostrando não só um grande controlo como também uma discriminação moral, religiosa e política, refletindo uma lógica de controlo social alargado e preventivo (Wang, 2019). Entre os visados estão, em primeiro lugar, aqueles com antecedentes penais relacionados com segurança pública, incluindo pessoas libertadas após cumprirem penas ou submetidas a medidas de controlo e vigilância[12], bem como os seus familiares. São também alvo de vigilância indivíduos que exerceram funções religiosas de forma não autorizada, como os imãs informais, ou que realizaram peregrinações, Hajj[13], sem aprovação estatal. Constam ainda nesta lista os seguidores de figuras consideradas ideologicamente perigosas pelas autoridades, especialmente aquelas associadas às chamadas "Seis Linhas", um grupo de pensadores islâmicos tidos como influentes. A lista inclui também comportamentos religiosos como partilhar ou receber conteúdo considerado *wahabita*[14], recolher com entusiasmo materiais para as mesquitas ou manter estilos de vida reservados, como evitar interações com vizinhos ou usar telemóveis analógicos. O regresso do estrangeiro, a recusa em participar em atividades organizadas pelo governo, e a mudança repentina de residência ou de comportamento também são motivos de inclusão. A vigilância estende-se a aspetos familiares, como o consumo elétrico anormal, violação da política de planeamento familiar, tendo mais filhos do que o permitido, e discrepâncias nos dados fornecidos durante visitas domiciliárias. É ainda monitorizado quem esteja desaparecido desde 2016 sem explicação registada, quem tenha solicitado passaporte sem notificar as autoridades locais, ou quem tenha registos biométricos e identitários incompatíveis.

Outros critérios dizem respeito a competências técnicas, como saber soldar ou fabricar explosivos, posse de dados suspeitos, como imagens ou comunicações cifradas e

[12] Segundo Wang (2019), as medidas de controlo e vigilância consistem em práticas utilizadas pelas autoridades chinesas para monitorizar e condicionar o comportamento dos cidadãos, especialmente em Xinjiang. Estas medidas incluem o uso de câmaras com reconhecimento facial, sistemas de análise de dados pessoais em tempo real, e plataformas como a IJOP, que cruzam informação sobre localização, consumo elétrico e comunicações. Um exemplo concreto é o programa Fanghuiju, que envolve visitas domiciliárias obrigatórias para recolha de dados sobre hábitos e crenças religiosas.

[13] Hajj é a peregrinação anual a Meca, considerada um dos cinco pilares do Islão. O Hajj representa um ato de devoção, purificação espiritual e união com a comunidade islâmica global (Al-Muntada Al-Islami Trust, 2024).

[14] Na RPC, o termo *wahabita* é frequentemente utilizado pelo PCC como rótulo para criminalizar práticas religiosas não sancionadas pelo Estado, mesmo que não haja ligação com extremismo violento. Assim, o rótulo *wahabita* serve, em muitos casos, como instrumento de repressão política e religiosa (Gonul & Rogenhofer, 2017).

codificadas, e até situações de perda de bens, deslocações não justificadas ou consumo energético fora do padrão. São também incluídos indivíduos ligados a redes criminais, pessoas sob vigilância especial, e qualquer outro perfil que, de forma arbitrária, as autoridades considerem suscetível de perturbar a "estabilidade social".

Este sistema de categorização é um dos pilares do modelo de governação preditiva e repressiva adotado pelo PCC, articulando a recolha massiva de dados, inteligência artificial e policiamento algorítmico com o objetivo de controlar o comportamento social em tempo real.

Embora se faça menção aos imãs, termo associado a uma posição de chefia dentro da religião, não são os únicos, discretamente mais visados, pelo PCC. Também os Uyghurs têm sido vítimas de detenções em massa, doutrinas políticas forçadas e restrições de manifestações políticas e religiosas, sendo que se estima que cerca de um milhão de pessoas pertencentes a estas minorias tenham sido detidas e mantidas por largos períodos em "campos de educação política"(Wang, 2019).

Constata-se, portanto, que o objetivo central desta aplicação, e da infraestrutura digital que a sustenta, é identificar padrões de comportamento quotidiano e formas de resistência por parte da população, com o propósito último de conceber e controlar a realidade social (Wang, 2019, p. 20). Esta lógica de atuação ocorre em claro prejuízo dos direitos e liberdades fundamentais dos cidadãos, incluindo a liberdade de expressão, associação, reunião e religião (Wang, 2019, p. 9).

A relevância do GSP para o DLP reside na sua capacidade de recolher e processar dados em tempo real a partir de múltiplas fontes, transformando-os em indicadores de risco.

Embora o contexto político chinês seja muito diferente do ocidental, a arquitetura técnica do GSP oferece um exemplo extremo de como os dados podem ser instrumentalizados no DLP. Ainda assim, a sua aplicação levanta questões profundas sobre ética, transparência, responsabilidade e respeito pelos direitos fundamentais

2.4.1.3. *Wechat*

A censura na internet na República Popular da China segue diretrizes rigorosas, com foco particular na restrição de conteúdos relacionados com ações coletivas de protesto, críticas a políticas governamentais e denúncias de corrupção. No entanto, também rumores e elementos associados a superstições são frequentemente censurados, uma vez que podem ser interpretados como formas de contestação social à narrativa promovida pelo governo (Tu, 2016).

Entre as plataformas digitais sob vigilância apertada, destaca-se o *WeChat*, uma aplicação multifuncional amplamente utilizada na China, que vai além das redes sociais tradicionais, integrando comunicação, pagamentos eletrónicos, acesso a serviços públicos e muito mais. Investigadores como Knockel et al. (2020) e Kenyon (2020) demonstram que os utilizadores do *WeChat* registados na RPC estão sujeitos a um sistema de censura política sistemática. Esta é aplicada principalmente por dois métodos: o primeiro é um mecanismo automatizado que, em tempo real, analisa o conteúdo textual em procura de palavras-chave proibidas e identifica imagens através da verificação do seu *hash*[15]; o segundo consiste numa verificação cruzada em sistemas partilhados, que compara conteúdos com bases de dados de imagens ou mensagens anteriormente classificadas como sensíveis. Para além da censura ativa de conteúdos, o PCC utiliza ainda estratégias subtis de controlo do espaço digital, nomeadamente através da amplificação da presença de meios de comunicação estatais nas plataformas digitais. Esta prática pretende garantir a disseminação da narrativa política oficial, enquanto reduz a visibilidade de conteúdos alternativos ou críticos, moldando assim a perceção pública e reforçando a estabilidade política (Tu, 2016).

Estas dinâmicas refletem um modelo de controlo digital profundamente enraizado nas lógicas do policiamento orientado por dados e do policiamento algorítmico, onde a monitorização não depende apenas de presença física ou vigilância clássica, mas de sistemas integrados de análise e filtragem de informação. A censura digital, neste contexto, funciona como um instrumento de gestão comportamental que antecipa e neutraliza potenciais dissidências, reforçando a autoridade do Estado sobre o ciberespaço (Knockel et al, 2020).

2.5.*Data Led Policing* em Portugal

O Conselho da União Europeia, através do n.º 2 do Art.º 2º da decisão nº 902 de 30 de novembro de 2009, define prevenção criminal de forma mais ostensivamente, no entanto mais precisa. Desta forma, "abrange todas as medidas destinadas a reduzir ou a contribuir para a redução da criminalidade e do sentimento de insegurança dos cidadãos, tanto quantitativo como qualitativamente, quer através de medidas diretas de dissuasão de atividades criminosas, quer através de políticas e intervenções destinadas a reduzir as

[15] O *hash* é uma sequência de caracteres associada a uma mensagem ou uma imagem, por exemplo, que garante a autenticidade, a singularidade e a integridade dessa mesma mensagem. Funciona assim como um identificador de algo para que este possa ser identificado por um determinado sistema (Hasan, 2022)

potencialidades do crime e as suas causas" (CUE, 2009, p. 2).

Abordando esta consideração sobre o próprio conceito de prevenção criminal, a CRP, através do n.º 3 do Art.º 272º, dita que a "prevenção dos crimes, incluindo a dos crimes contra a segurança do Estado, só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos", vindo aqui realçar os limites, sendo estes os direitos, liberdades e garantias dos cidadãos, da prevenção criminal.

Também a Lei n.º 49/2008, de 27 de agosto, Lei de Organização da Investigação Criminal (LOIC), pela alínea b) do n.º 4 do Art.º 3º atribui a competência aos órgãos de polícia criminal (OPC) de "desenvolver as acções de prevenção e investigação da sua competência ou que lhes sejam cometidas pelas autoridades judiciárias competentes". Fazendo referência, também, à Lei n.º 51 /2023, de 28 de Agosto, a Lei de Política Criminal – Biénio 2023-2025, no n.º 1 do Art.º 9º, está explícito que "na prevenção da criminalidade, as forças e os serviços de segurança desenvolvem programas e planos de segurança comunitária e de policiamento de proximidade destinados a proteger as vítimas especialmente vulneráveis e a controlar as fontes de perigo referentes às associações criminosas e organizações terroristas, aos meios especialmente perigosos, incluindo armas de fogo, químicas, biológicas, radiológicas e nucleares ou engenhos ou produtos explosivos, e aos meios especialmente complexos, como a informática e a Internet".

Abordando a questão do tratamento e do uso dos dados pessoais nas demais plataformas de intercambio de informações, como a Plataforma de Intercâmbio de Informação Criminal (PIIC) e o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), é necessário analisar a Lei n.º 59/2019, de 8 de agosto, que, transpondo a Diretiva 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, "estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" (art. 1º da Lei n.º 59/2019).

No art. 6º, n.º 1 al. b), é explicito que o tratamento de categorias especiais de dados, nomeadamente "dados genéticos, dos dados biométricos destinados a identificar uma pessoa singular de forma inequívoca" (art. 6º, n.º 1 da Lei n.º 59/2019), pode ser efetuado se "destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular". A

única referencia que se faz em alguma diploma legal aos "interesses vitais" é no Regulamento 679/2016 do Parlamento Europeu e do Conselho de 27 de abril de 2016, denominado de Regulamento Geral de Proteção de Dados (RGPD), na sua 46º consideração que dita que o tratamento de dados pessoais com "base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico", deixando apenas esta exceção, restrita, que deve ser justificada em casos em que não existam mais alternativas legais para o tratamento dos dados.

Denotamos a profundidade deste diploma ao abordar, no seu art. 8º n.º 4, a questão da cooperação judiciária e policial no âmbito da União Europeia, em que fica sanado que as condições aplicáveis às autoridades e organismos de cooperação internacionais não divergem das condições impostas às FS e SIIC nacionais.

Portugal, atualmente, está colocado na 7ª posição do *Global Peace Index*. Não obstante de ser um resultado positivo, é necessário analisar os anos subsequentes. Em 2020, Portugal estava colocado no 3º lugar, sendo o primeiro país da União Europeia, em 2021, em 4º colocado, em 2022 em 6º e em 2023 e 2024, apresenta-se em 7º colocado. Analisando ainda os relatórios do *Global Peace Index*, observamos que em todos os anos referidos, excetuando 2024, o nível global de paz deteriorou-se 0.34, 0.07, 0.3 e 0.42, respetivamente, apenas sendo positivos, 0.56 pontos percentuais em 2024. Retiramos daqui essencialmente que embora a paz global tenha vindo a deteriorar-se ao longo dos últimos anos, em virtude das instabilidades do panorama político mundial, Portugal tem acompanhado essa deterioração, no entanto não se excedendo negativamente em comparação aos seus pares, estando em 4º da União Europeia e 16 lugares acima do país que faz fronteira, Espanha.

Apesar de se considerar Portugal como um país seguro, em termos de perceção de segurança, Portugal, segundo o *Safety Perceptions Index 2023*, surge na 80º posição, de 121 países abrangidos pelo estudo.

Relativamente a *SC*, Portugal faz parte de um projeto, denominado de *Horizon 2020*, que pretendeu implantar em determinas estratégias-piloto de forma a averiguar a potencialidade de exponenciar determinadas cidades, e torná-las em *SC*. Foram selecionas em Portugal duas cidades, Lisboa e Évora, como cidades piloto, em que implantou medidas como edifícios energeticamente eficientes, utilização de fontes de energia renováveis e governação urbana e participação dos cidadãos. Foram implantadas, de forma global, 77% das ideias como estavam comtempladas até ao final do tempo do projeto sendo apontados como principais obstáculos a falta de financiamento, entraves regulamentares e a falta de sustentabilidade do modelo de negócio (TCE, 2023)

Apesar da pouca presença de elementos de SC em Portugal, já existem registados 42 *DC*, fundamentais para o suporte do setor digital que envolve telecomunicações, finanças e administração pública (*Data Centers Map*, 2025).

2.5.1. Videovigilância em Portugal

A legislação, relativa à videovigilância em Portugal, é caracterizada em dois períodos distintos. O primeiro de 2005 a 2012, demarcado por uma legislação mais restritiva, que atribuía um papel privilegiado à Comissão Nacional de Proteção de Dados, obrigando a que os pedidos contivessem dados precisos sobre a proporcionalidade, necessidade e adequação dos sistemas de vigilância. Após este período, demarcado por um número elevado de pareceres e decisões negativas tentando-se ressalvar ao máximo o direito à privacidade, inicia-se um período que dinamiza todo este processo, caracterizado pela desvinculação dos pareceres da Comissão Nacional de Proteção de Dados (CNPD) e pela não obrigação de apresentar provas de riscos objetivos para a segurança nos pedidos redigidos (Melo & Viseu, 2024).

A partir de 2021, com a Lei n.º 95/2021, denota-se um aumento dos pedidos de instalação de câmaras em espaços públicos, com um total de 11 localidades com sistemas de vigilância em funcionamento e cinco localidades autorizadas a utilizá-lo, mas ainda inativas.

Relativamente à transparência do processo, Melo & Viseu, (2024), afirmam que há quatro aspetos fundamentais menosprezados. O primeiro aspeto que se pretende ressalvar é que desde 2018, todos os despachos autorizam o funcionamento ininterrupto dos sistemas e a gravação de som "sempre que se verifique uma situação de perigo concreto para a segurança de pessoas e bens" (Melo & Viseu, 2024, p. 11). O segundo ponto é a quantidade de camaras aprovadas que se encontra inexistente em alguns despachos, nomeadamente no caso do Bairro Alto e da Amadora. Relativamente à localização das mesmas Melo & Viseu, constataram que em apenas 22,2% dos despachos se indica a localização exata das câmaras.

Por fim, também as características das câmaras são negligenciadas, não sendo mencionadas em nenhum despacho, não podendo deste modo analisar a sua conformidade com os preceitos legais (Melo & Viseu, 2024).

Sendo que o Art.º 7.º da Lei n.º 95/2021 dita explicitamente que a autorização deve conter os locais abrangidos pelo sistema de videovigilância, as limitações e condições do uso do sistema, a proibição de captação de sons, com a devida exceção, o tipo de câmaras e as suas especificações, denota-se um próprio incumprimento da Lei por parte da entidade que autoriza o uso do sistema de videovigilância.

Melo e Viseu (2024) consideram que o uso exacerbado e expansionista da videovigilância merece em primeiro lugar maior transparência no seu propósito e nos seus objetivos, que se têm sido obscurecidos por presunções e perceções, por vezes discriminatórias, no que concerne igualmente à criminalidade. Serve de exemplo problemático do referido anteriormente o caso da Amadora, zona alta densidade populacional, maioritariamente de estratos socioeconómicos mais baixos e de pessoas racializadas, onde não se encontra explanado a localização dos equipamentos e o tipo de câmaras que estão a ser utilizadas pela Divisão Policial da Amadora da Polícia de Segurança Pública.

PARTE 2 - ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO 3 – METEDOLOGIA

Após realizado o enquadramento teórico, apresenta-se o capítulo que versa sob a metodologia, dividido em cinco subcapítulos, que dão respostas aos métodos e técnicas utilizadas nesta investigação.

A investigação científica caracteriza-se como um processo sistemático que visa a obtenção de conhecimento estruturado e logicamente ordenado. O principal objetivo é fornecer informações que contribuam para a resolução de problemas, por forma a responder a questões por um meio científico (Haro et al., 2016). É nesse contexto que a metodologia da investigação assume um papel central na estruturação do estudo, sendo fundamental para identificar os problemas a serem analisados e alcançar os objetivos e para alcançar os objetivos propostos. A metodologia compreende um conjunto de métodos, técnicas de recolha e análises de dados, que deverão ser compatíveis com a investigação.

Desta forma a metodologia desempenha um papel crucial na organização dos passos necessários para a obtenção de conhecimento científico e na validação dos resultados obtidos (Kilani & Kobziev, 2016), adotando deste modo, o estudo de caso como estratégia metodológica principal, dada a necessidade de compreender um fenómeno complexo de forma integrada com o seu contexto específico.

3.1. Formulação dos objetivos e questões de investigação

Após enunciados os objetivos gerais e específicos e partindo da Q_P expressa na introdução, "Qual o impacto da utilização do Data Led Policing, no âmbito da prevenção criminal na República Popular da China?" afunilamos a investigação para as seguintes questões derivadas (**Q_D**):

- **Q_{D1}**: Como é que o *Data Led Policing* é utilizado na República Popular da China?
- **Q_{D2}**: Quais são os contributos do *Data Led Policing* na atividade policial?
- **Q_{D3}**: Como é que o *Data Led Policing* poderá ser utilizado em Portugal?

Para melhor ilustração, encontra-se em baixo, uma tabela que demonstra a relação entre os objetivos específicos e as questões derivadas.

O_G: Analisar o impacto da utilização do *Data Led Policing* na Prevenção Criminal na RPC.	**Q_P: Qual o impacto da utilização do *Data Led Policing*, no âmbito da Prevenção Criminal na República Popular da China?**
O_{E1}: Analisar o *Data Led Policing* na Prevenção Criminal da RPC;	**Q_{D1}:** Como é que o *Data Led Policing* é utilizado na República Popular da China?
	Q_{D2}: Quais são os contributos do *Data Led Policing* na atividade policial?
O_{E2}: Analisar a aplicabilidade e os desafios do Data Led Policing em Portugal.	**Q_{D3}:** Como é que o *Data Led Policing* poderá ser utilizado em Portugal?

Tabela n.º 4: Relação entre Objetivos e Questões

Fonte: Elaboração Própria

3.2. Método de Abordagem e Desenho de pesquisa

Segundo Rosado, "os paradigmas orientam as metodologias, as metodologias enformam e aferem os métodos e os métodos constituem um conjunto de técnicas que determinam o sentido orientador de uma investigação" (2017, p. 119). Assim compreende-se a necessidade real de identificar o paradigma que se caracterizará como sociocrítico, que embora se descreva como essencialmente qualitativo e "ligado a um interesse crítico emancipatório" (Rosado, 2017, p. 119), pode conter dados qualitativos para sustentar padrões, por exemplo.

É sabido que "métodos constituem um conjunto de técnicas que determinam o sentido orientador de uma investigação" (Rosado, 2017, p. 119), sendo possível identificar: o indutivo, o dedutivo e o hipotético-dedutivo. Neste estudo foi adotado o método dedutivo que assenta numa lógica que parte de uma ou de várias opções teóricas tendo em vista

explicar um fenómeno particular (Rosado, 2017). Esta investigação segue um método qualitativa. Segundo (Reis et al.), "Esta opção justifica-se pela necessidade de investigar um fenómeno contemporâneo no seu contexto do mundo real" (2022, p. 3).

O tipo de estudo adotado foi o estudo de caso, que segundo Robert Yin "é um inquérito empírico que investiga um fenómeno contemporâneo no seu contexto de vida real, especialmente quando as fronteiras entre o fenómeno e o contexto não são claramente evidentes" (Yin, 2003, p. 13).

A tabela seguinte apresenta uma perspetiva geral do método utilizado nesta investigação.

Método	Fonte de Dados	Descrição do Método	Contributo para a investigação
Dedutivo	Entrevistas semiestruturadas, documentos oficiais, legislação e literatura científica.	Estuda a aplicação do DLP em contexto real, com base em entrevistas (10) a especialistas e análise documental.	Este método permite validar empiricamente os pressupostos teóricos e gerar contributos aplicáveis à realidade portuguesa no domínio da segurança interna.

Tabela 5: Síntese metodológica desta investigação

Fonte: Elaboração própria

3.3. Métodos de recolha de dados

De acordo com Fortin (2009), a escolha dos métodos de recolha de dados deve assegurar a ampliação do conhecimento sobre o tema em estudo, proporcionando uma base sólida para a fundamentação dos resultados obtidos.

Esta investigação estrutura-se em duas partes principais: a primeira dedicada ao enquadramento teórico e a segunda ao enquadramento metodológico e à análise e discussão dos resultados. Na fase inicial, referente à componente teórica, foi realizada uma pesquisa documental com recurso a fontes primárias e secundárias. As fontes primárias incluíram legislação pertinente, relatórios anuais e índices internacionais, enquanto as fontes secundárias abrangeram livros, artigos científicos e dissertações académicas.

A pesquisa documental desempenhou um papel fundamental na clarificação dos conceitos-chave relacionados com o objeto de estudo, bem como na identificação de lacunas na literatura existente, permitindo uma definição precisa das questões de investigação e um enquadramento teórico rigoroso (Fortin, 2009; Quivy & Campenhoudt, 2019). As fontes bibliográficas foram consultadas tanto em bibliotecas físicas como em acervos digitais e repositórios comuns como o *Scopus*, a *EBSCO*, o RCAAP, *Web of Science* e *Google Scholar*,

garantindo uma abordagem abrangente e atualizada da temática em análise. Do número total de artigos científicos, 37, apenas 12 são do segundo quartil, ou seja 32,43%, sendo que os restantes estão enquadrados no primeiro quartil, 67.57%, como demonstrando em tabela em apêndice-A. Na ilustração seguinte apresenta-se um gráfico organizado em intervalos de 2 anos, que apresenta os artigos científicos Q1 e Q2 nos respetivos anos.

Ilustração n.º 3 – Número de Artigos Científicos por quartil em intervalos de 2 anos

Fonte: Elaboração Própria

A utilização de entrevista no presente estudo de caso justifica-se pela sua capacidade de proporcionar uma compreensão aprofundada e contextualizada do fenómeno em análise. De acordo com Yin (2018), as entrevistas são uma ferramenta essencial na investigação qualitativa, especialmente em estudos de caso, uma vez que permitem explorar em detalhe as perceções, experiências e perspetivas dos participantes.

Ao possibilitar uma interação direta com os envolvidos, as entrevistas apresentam-se como uma fonte de dados primários, que não poderiam ser obtidos através de outros métodos quantitativos ou de fontes secundárias. Os entrevistados são indivíduos conhecedores da temática que tiveram ou têm um papel preponderante no tema abordado e por isso são considerados relevantes para a investigação.

Segundo Yin (2018), as entrevistas são especialmente apropriadas em estudos de caso, permitindo aceder diretamente às perceções, experiências e raciocínios dos participantes, sobretudo quando se procura explorar fenómenos complexos e contextualmente situados. Neste sentido, este instrumento revelou-se essencial para abordar a diversidade de perspetivas sobre a viabilidade, adaptação, impacto e limites éticos da adoção do DLP em Portugal.

O guião de entrevista foi elaborado com base nos objetivos específicos da

investigação, articulando-se com as questões derivadas. As cinco perguntas formuladas incidiram sobre: i) a possibilidade de aplicação do DLP nos moldes chineses em Portugal; ii) os ajustes necessários à realidade nacional; iii) os contributos esperados para a segurança interna; iv) as comparações com os sistemas de videovigilância existentes; e v) os desafios éticos, legais e operacionais que uma eventual implementação poderá enfrentar. As mesmas concorreram essencialmente para dar resposta ao O_{E2} que se traduz em "Analisar a aplicabilidade e os desafios do Data Led Policing em Portugal", e consequente Q_{D3} que questiona "Como é que o Data Led Policing poderá ser utilizado em Portugal?". O guião utilizado na realização destas entrevistas encontra-se no apêndice-B, assim como toda a documentação que o acompanha

A seleção dos participantes seguiu um critério de relevância temática e diversidade institucional. Foram entrevistados profissionais com responsabilidades ou experiência direta nos domínios da segurança interna, policiamento, sistemas de vigilância e inteligência. Esta amostragem intencional garantiu que os dados recolhidos fossem ricos em conteúdo, oferecendo uma base sólida para a análise qualitativa subsequente.

As entrevistas foram conduzidas em ambiente reservado, com consentimento informado dos participantes, respeitando os princípios éticos da investigação científica e as orientações da APA, 7.ª edição, fazendo-se acompanhar de uma carta de apresentação, esclarecendo os objetivos do estudo e garantido o anonimato dos entrevistados. Todas as entrevistas foram gravadas pelo gravador do telemóvel, transcritas integralmente pelo *software TurboScribe* e validadas posteriormente pelos próprios entrevistados, assegurando a fidelidade das informações.

3.4. Métodos e técnicas de amostragem

A presente investigação recorre ao estudo de caso como estratégia metodológica central, atendendo à necessidade de compreender um fenómeno complexo em articulação com o seu contexto específico. De acordo com Yin (2018), o estudo de caso é particularmente apropriado quando se pretende analisar fenómenos contemporâneos inseridos em contextos reais, sobretudo quando os limites entre o fenómeno em si e o ambiente envolvente são ténues ou indefinidos. A escolha desta abordagem foi ainda reforçada pelo facto de o objeto de estudo representar uma situação específica e potencialmente crítica, na medida em que envolve a transposição de um modelo de policiamento aplicado na RPC para um contexto democrático europeu, Portugal, levantando questões técnicas, éticas e políticas singulares.

Optou-se por uma abordagem exploratória, tendo em conta que o objetivo principal da investigação é compreender em profundidade como o modelo DLP poderá ou não ser adaptado à realidade portuguesa, mais do que testar hipóteses pré-estabelecidas.

Quanto à técnica de amostragem, foi utilizada uma amostragem não probabilística intencional, pois foram escolhidos elementos da população para pertencerem à amostra, por serem representativos e por conhecerem características especificas do que se pretende estudar (Sarmento, 2013). Esta técnica permite selecionar participantes com base na sua experiência, conhecimento ou posição institucional relevante para o objeto de estudo. Assim, foram incluídos dez profissionais e especialistas com intervenção direta nas áreas da segurança interna, policiamento, sistemas de vigilância, políticas públicas e do garantindo que as respostas obtidas fossem informadas e pertinentes.

O objetivo foi garantir uma abordagem multidimensional ao fenómeno do Data Led Policing (DLP), possibilitando o confronto entre diferentes olhares sobre a sua viabilidade, aplicabilidade e implicações no contexto português, tendo como pano de fundo o modelo desenvolvido na RPC.

Na tabela 6, com a caracterização sumária dos entrevistados, respeitando os critérios de identificação relevantes para o enquadramento analítico, mas assegurando a confidencialidade sempre que solicitada, a apresentação dos entrevistados.

Código	Perfil	Área
E1	Académico/Política Internacional	Relações Internacionais
E2	Político/Institucional	Segurança e Administração Interna
E3	Político/Institucional	Segurança e Administração Interna
E4	Político/Institucional	Direito e Administração Interna
E5	Político/Institucional	Coordenação e Estratégia de Segurança Interna
E6	Jurídico/Académico	Direito e Relações Internacionais
E7	Académico/Geopolítico	Relações Internacionais e Segurança
E8	Académico/Geopolítico	Estudos Chineses e Geopolítica
E9	Académico/Técnico	Engenharia Informática, e Sistemas de Apoio à Decisão
E10	Académico/Internacional	Estudos Chineses, Relações Internacionais e Diplomacia Pública

Tabela 6: Relação de Entrevistados, Perfil e Área

Fonte: Elaboração Própria

3.5. Técnicas de tratamento e análise de dados

No que concerne às técnicas de recolha de dados, "é sabido que, ao nível das técnicas de recolha de dados em ciências sociais, se incluem as técnicas documentais e as técnicas não documentais" (Rosado, 2017, p. 124). O uso de técnicas documentais decorre desta investigação, "necessitar de dados macrossociais, que apenas organismos oficiais poderosos, como os institutos nacionais de estatística, têm condições para recolher" (Quivy and Campenhoudt, 1995, p. 201).

A utilização das bases de dados como *Scopus* e *Web of Science* para esta pesquisa justifica-se pela sua reconhecida qualidade e credibilidade na comunidade científica. Ambas as plataformas indexam revistas científicas e artigos que passam por um rigoroso processo de avaliação por pares, *peer-review*, o que assegura a fiabilidade e a relevância das fontes consultadas. A escolha dessas bases permite o acesso a conteúdos científicos validados e de alto nível, fundamentais para a fundamentação e desenvolvimento do estudo, garantindo a qualidade e a precisão dos resultados obtidos.

A análise das informações recolhidas nas entrevistas foi realizada segundo as etapas enunciadas por Guerra (2006), que comportam a transcrição, a leitura, elaboração de sinopses, análise descritiva e interpretação. As subcategorias das respostas foram criadas com suporte da análise da bibliografia em conjunto com as respostas que foram sendo obtidas. Deste modo, permite-se que a investigação seja conduzida de forma clara, favorecendo uma melhor e aprofundada interpretação dos dados qualitativos, obtendo-se uma análise crítica fundamentada, alinhada com o enquadramento teórico e com os objetivos da investigação.

CAPÍTULO 4 - ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1. Método de análise de conteúdo

Este capítulo apresenta a análise e discussão dos resultados obtidos através das entrevistas realizadas no âmbito do estudo. Após a transcrição integral das entrevistas, procedeu-se à identificação e seleção dos conteúdos mais relevantes para os objetivos da investigação.

A apresentação dos resultados será realizada questão a questão, promovendo a articulação entre os diferentes contributos dos participantes e as referências teóricas previamente abordadas. Este procedimento visa não apenas descrever as perceções recolhidas, mas também discuti-las criticamente à luz do quadro conceptual da investigação,

de modo a avaliar a pertinência, os limites e os desafios da aplicação do DLP no contexto português, com referência ao modelo adotado pela RPC.

4.2. Resultados

As respostas dos entrevistados foram codificadas e organizadas em categorias de análise que permitem uma leitura aprofundada das tendências e divergências identificadas. Para complementar e reforçar a transparência metodológica, encontra-se em apêndice uma tabela de análise de entrevistas, Apêndice-C onde são apresentadas de forma sistematizada as respostas e os códigos atribuídos a cada entrevistado, facilitando a compreensão detalhada dos dados tratados.

A análise da primeira questão, centrada na possibilidade de aplicar o modelo de DLP, tal como implementado na RPC, ao contexto português, revelou um consenso entre os entrevistados. Nove dos dez participantes consideraram inviável essa transposição, apontando incompatibilidades profundas de ordem estrutural, legal e cultural. O E2 salientou que estamos perante regimes políticos e jurídicos radicalmente distintos e destacou os limites legais impostos em Portugal à utilização de ferramentas de monitorização. O E6 reforçou que a realidade portuguesa, enquanto Estado de Direito Democrático, inviabiliza qualquer tentativa de replicar diretamente o modelo chinês. Outros entrevistados, como o E9 e o E8, sublinharam que, embora as tecnologias possam ser tecnicamente replicadas, os princípios normativos e culturais em Portugal tornam tal aplicação impraticável e eticamente inaceitável.

A análise destas entrevistas permitiu concluir que existe uma rejeição quase unânime da aplicabilidade direta do modelo da RPC em Portugal, sendo esta rejeição sustentada por argumentos legais, éticos e institucionais. Assim, 90% dos entrevistados consideram inviável a transposição direta do DLP para o contexto português.

A segunda questão explorou a viabilidade de adaptar elementos do modelo da RPC ao contexto português. A maioria dos entrevistados manifestou ceticismo quanto à possibilidade de uma adaptação bem-sucedida, realçando que o problema não reside apenas na tecnologia, mas nos fins e lógicas de governação que sustentam o modelo. O E1 e o E2 rejeitaram a hipótese de uma adaptação, sublinhando a necessidade de garantir o respeito absoluto pelos direitos fundamentais. O E3 reconheceu que qualquer adaptação sofreria tantas alterações que acabaria por se afastar radicalmente do modelo original, sugerindo antes a aplicação seletiva de ferramentas específicas em áreas como a cibercriminalidade e o terrorismo. Outros, como o E6 e o E4, admitiram que se poderiam retirar aprendizagens

tecnológicas do modelo chinês, desde que submetidas a fortes salvaguardas legais e democráticas.

A reflexão crítica evidencia que, embora exista margem para incorporar certas inovações tecnológicas de forma controlada, não há viabilidade para importar o modelo enquanto sistema. Apesar de pequenas possibilidades de inspiração tecnológica, 80% dos entrevistados expressaram reservas profundas quanto à adaptação substancial do DLP ao contexto nacional.

A terceira questão procurou avaliar de que forma o DLP, adaptado à realidade portuguesa, poderia contribuir para a segurança interna. Aqui surgiu uma maior divergência entre os entrevistados. O E6 destacou que a recolha e articulação eficiente de dados pode melhorar a capacidade de resposta das FS, enquanto o E10 apontou que as tecnologias como o reconhecimento facial e os sistemas integrados de IA poderiam ter um efeito dissuasor e aumentar a sensação de segurança no espaço público. No entanto, estas perspetivas mais otimistas foram contrabalançadas por opiniões como a do E5, que alertou para o risco de erosão da confiança pública, e do E7, que enfatizou os perigos associados à opacidade na gestão dos dados. O E1 sugeriu que seria mais produtivo aprender com modelos europeus em vez de adaptar soluções oriundas da RPC. A análise comparativa revelou que, apesar de haver algum reconhecimento quanto ao potencial operacional do DLP, predominam as reservas éticas e legais. Assim, cerca de 60% dos entrevistados apontaram potencialidades específicas, mas todos frisaram a necessidade de uma implementação muito cautelosa e controlada.

A quarta questão procurou analisar as semelhanças entre o modelo de videovigilância atualmente existente em Portugal e o DLP da RPC. Todos os entrevistados concordaram que, embora existam semelhanças superficiais a nível tecnológico, os dois modelos diferem profundamente em termos de objetivos, amplitude e enquadramento legal. O E5 destacou que em Portugal a videovigilância é regulamentada e limitada pela legislação nacional e europeia, contrastando com a lógica intrusiva da RPC, que visa igualmente obter o controlo social. O E1 reforçou que as limitações jurídicas portuguesas, como a proibição de captação de som e as restrições ao acesso a imagens, distanciam o sistema português do modelo da RPC. Outros entrevistados, como o E6, reconheceram que tecnologias como o reconhecimento facial poderão ser integradas no futuro, mas apenas em moldes muito restritos e com plena aceitação social. O que se retira desta questão é que, como sublinhado por todos os entrevistados, as diferenças estruturais entre os modelos são profundas e qualquer aproximação tecnológica deverá respeitar os valores democráticos e a

proporcionalidade legal.

Por fim, a quinta questão identificou os principais desafios que Portugal enfrenta para adotar um modelo inspirado no DLP. A esmagadora maioria dos entrevistados apontou os entraves jurídicos e constitucionais como o maior obstáculo. O E5 e o E6 destacaram os desafios legais impostos pelo RGPD e a necessidade de capacitação institucional e técnica, enquanto o E1 e o E4 sublinharam as resistências culturais ligadas à memória histórica do Estado Novo. Além disso, os entrevistados referiram problemas de interoperabilidade entre sistemas e a fragmentação institucional como barreiras significativas à implementação de qualquer sistema avançado de análise de dados. Foi possível concluir que, para além das dificuldades tecnológicas e operacionais, há uma consciência clara sobre os limites éticos e políticos que moldam qualquer tentativa de avanço neste domínio. Todos os entrevistados identificaram pelo menos um desafio estrutural relevante, como o enquadramento jurídico e constitucional rigoroso, aceitação social e confiança dos cidadãos, a escassez de recursos humanos e formação especializada, a fragmentação institucional e falta de interoperabilidade e os riscos de erosão democrática e ausência de supervisão robusta, reforçando a ideia de que a adoção de ferramentas inspiradas no DLP deve ser gradual, transparente e juridicamente sólida.

Da realização destas entrevistas retira-se essencialmente que o DLP da RPC não é transponível para Portugal em termos diretos devido às profundas diferenças legais, políticas e culturais, no entanto, existe alguma margem para incorporar certos elementos tecnológicos, desde que submetidos a rigorosas salvaguardas democráticas e jurídicas.

4.3. Discussão dos resultados

A presente discussão de resultados organiza-se em torno das três questões derivadas e da questão de partida, proporcionando uma reflexão crítica e aprofundada sobre o modelo de DLP implementado na RPC e a sua eventual aplicabilidade ao contexto português. Este subcapítulo integra o quadro teórico delineado na Parte I com os contributos recolhidos nas entrevistas realizadas, tendo como objetivo responder de forma fundamentada à questão geral que orienta esta investigação, a qual pretende compreender em que medida o modelo de DLP da RPC pode ser analisado e avaliado para aplicação na realidade portuguesa.

No que diz respeito à Q_{D1}, a investigação sobre a utilização do DLP na RPC revela uma implementação solidamente enraizada numa lógica de governação autoritária e vigilância extensiva. Estudos como os de Liang e Chen (2022) e Wang (2019) evidenciam a recolha centralizada de grandes volumes de dados, incorporando tecnologias IA, *Big Data* e

sistemas biométricos de vigilância. Tanto a análise bibliográfica como as entrevistas realizadas convergem na perceção de que este modelo é incompatível com os princípios fundamentais de um Estado de direito democrático. Como é realçado pelo conteúdo das entrevistas, o DLP é um sistema altamente centralizado e tecnologicamente avançado, fortemente assente na recolha e análise massiva de dados, que integra uma vasta rede de videovigilância, sistemas de reconhecimento facial, algoritmos preditivos e plataformas de *Big Data* que operam em articulação com diversas bases de dados governamentais. O DLP na RPC visa sobretudo a antecipação de comportamentos considerados de risco, funcionando como um instrumento de prevenção criminal, mas também de controlo social alargado. O sistema permite às autoridades monitorizar em tempo real grandes segmentos da população, identificando padrões de comportamento considerados desviantes com base em critérios algorítmicos.

O E2 sublinha, por exemplo, que este modelo "não é compatível com a nossa realidade institucional", enquanto o E6 reforça a ideia de que a RPC opera "um modelo centralizado e autoritário". Esta convergência entre a literatura e os entrevistados mostra um consenso firme quanto à inviabilidade de uma transposição direta do modelo da RPC para Portugal. Contudo, observa-se uma nuance importante. A análise bibliográfica, nomeadamente Fontes et al. (2022) destacam primordialmente a eficácia tecnológica deste modelo e sublinham a sofisticação dos sistemas de IA integrados em dispositivos de vigilância pública. Por outro lado, os entrevistados enfatizam as implicações éticas e jurídicas do modelo, refletindo uma visão crítica mais enraizada nos valores democráticos europeus, em linha com as preocupações levantadas por Brayne (2017) sobre os riscos de vigilância excessiva, e por Babuta (2017), que alerta para os desafios legais e a necessidade de proteção dos direitos fundamentais., ao passo que os entrevistados enfatizam as implicações éticas e jurídicas, refletindo uma visão crítica mais enraizada nos valores democráticos europeus. O E4, por exemplo, descreve o modelo da RPC como "um policiamento preditivo extremo", alertando para dimensões éticas que nem sempre são suficientemente aprofundadas nos estudos técnicos.

Relativamente à QD2, os contributos do DLP para a atividade policial na RPC são amplamente reconhecidos, tanto em estudos académicos como nas entrevistas realizadas. Autores como Wu et al. (2021) e Liang e Chen (2022) destacam o impacto e a aplicação de tecnologias avançadas que aumentam significativamente a capacidade preditiva e operacional das FS. Os entrevistados reconhecem que o modelo de DLP pode trazer contributos operacionais relevantes, como o reforço da capacidade preditiva, maior rapidez

na identificação de suspeitos e uma gestão mais eficiente dos recursos policiais. Esta realidade foi também referida por entrevistados como o E10, que salientou a eficácia da identificação em tempo real, e pelo E6, que partilhou uma experiência pessoal de reconhecimento facial automático em Pequim. No entanto, sublinham que esses benefícios só seriam aceitáveis se integrados num quadro legal e ético rigoroso, com controlo judicial e respeito pelos direitos fundamentais. A revisão de literatura, por outro lado, tende a valorizar mais os ganhos tecnológicos e operacionais do modelo, destacando a sofisticação dos sistemas de IA e a eficácia na prevenção criminal. Assim, enquanto a literatura prioriza o potencial técnico, os entrevistados realçam os riscos e condicionantes associados à sua aplicação em contextos democráticos.

No que concerne à QD3, a viabilidade de aplicação de elementos do DLP no contexto português suscitou respostas mais variadas e fragmentadas. Considera-se que a aplicação do modelo DLP só seria viável de forma parcial e profundamente adaptada. Os contributos tecnológicos do DLP, como o cruzamento de dados e as análises preditivas, poderiam ser aproveitados, mas apenas se integrados em sistemas transparentes, com salvaguardas legais robustas e supervisão independente. Destaca-se os riscos de erosão de direitos fundamentais e a necessidade de compatibilizar qualquer inovação com os valores democráticos e o quadro jurídico nacional.

A literatura consultada não oferece soluções explícitas para realidades democráticas como a portuguesa, mas os entrevistados forneceram perspetivas concretas e valiosas. Há um consenso claro quanto à impossibilidade de importar o modelo na sua totalidade, como destacaram o E1 e o E2. No entanto, surgem propostas para adaptar certos aspetos tecnológicos de forma seletiva, especialmente para áreas de maior risco, como sugerido pelo E3, que mencionou a potencial utilização controlada de *Big Data* na prevenção de crimes como o terrorismo e a cibercriminalidade. O E6 acrescentou uma proposta inovadora, defendendo que, em vez de se pensar num "modelo" fechado, se deve procurar uma "inspiração tecnológica", assegurando que qualquer adaptação seja sempre acompanhada de salvaguardas democráticas rigorosas.

A investigação evidencia também contradições relevantes no debate sobre o impacto potencial da tecnologia. Entrevistados como o E10 realçaram os benefícios na melhoria da perceção pública de segurança e na rapidez de resposta policial, enquanto outros, como o E5 e o E7, manifestaram preocupações sérias quanto aos riscos de erosão da confiança pública e da liberdade individual. Este contraste salienta uma tensão estrutural entre a ambição tecnológica e a preservação dos direitos fundamentais, que se revela um dos principais

desafios na ponderação de políticas públicas neste domínio.

A ausência de interoperabilidade entre sistemas de segurança e a falta de uma estratégia integrada foram destacadas como obstáculos operacionais e institucionais por vários entrevistados. O E4, por exemplo, apreciou o que considera uma abordagem demasiado restritiva à videovigilância, embora reconhecendo a necessidade de manter um equilíbrio prudente entre eficácia e respeito pelos direitos dos cidadãos.

Ao retomar a questão de partida, torna-se claro que esta investigação demonstra que o modelo de DLP da RPC, embora constitua um exemplo paradigmático de policiamento digital e vigilância preditiva, não pode ser replicado integralmente em Portugal devido às profundas divergências políticas, culturais e jurídicas que os dois países apresentam. A essência autoritária e altamente intrusiva do modelo da RPC está em desacordo com os princípios democráticos que estruturam o Estado português e o seu ordenamento jurídico. Não obstante, os resultados também evidenciam que existe potencial para adaptar determinadas tecnologias e procedimentos do DLP ao contexto nacional, desde que este processo seja rigorosamente balizado por princípios como a proporcionalidade, a legalidade e a supervisão democrática.

CONCLUSÕES

A presente investigação teve como objetivo a análise da utilização do DLP na prevenção criminal, mais concretamente na RPC, e posterior análise da viabilidade e os impactos da aplicação do modelo de DLP em Portugal.

Partindo da questão de partida e das três questões derivadas, esta investigação procurou oferecer uma visão crítica e aprofundada sobre os desafios e potencialidades da eventual adoção deste modelo em contexto democrático, cruzando a revisão de literatura com os testemunhos de especialistas entrevistados.

Relativamente à Q_{D1}, conclui-se que o modelo do DLP da RPC assenta numa lógica centralizada de controlo social, através da integração de sistemas de videovigilância, reconhecimento facial e algoritmos preditivos, orientados para a monitorização contínua da população.

No que diz respeito à Q_{D2}, foram identificados benefícios relevantes ao nível da capacidade preditiva, eficiência na gestão de recursos e rapidez na resposta das FS. Contudo, esses ganhos operacionais só seriam admissíveis, em contextos democráticos, se acompanhados por mecanismos robustos de controlo legal e respeito pelos direitos fundamentais. A investigação destacou ainda que as potencialidades operacionais do DLP, como o reforço da capacidade preditiva e a utilização de tecnologias de IA, podem contribuir para melhorar a eficácia e eficiência das FS. Contudo, foram identificadas preocupações relevantes relativamente aos riscos éticos e sociais associados a modelos de policiamento excessivamente intrusivos, nomeadamente a erosão da confiança pública e a ameaça às liberdades civis.

Relativamente à Q_{D3}, que se debruça sobre a utilização e aplicabilidade do DLP em Portugal, verificou-se que apenas uma adoção parcial e adaptada seria viável. Elementos tecnológicos como o cruzamento de dados e análises preditivas podem ser aproveitados, desde que integrados num sistema transparente, com maior interligação interinstitucional, com supervisão independente e conforme com os princípios constitucionais.

Procurando dar resposta à $Q_{P,}$ através da análise teórica e empírica, verificou-se que o DLP na RPC é fortemente sustentado por um modelo autoritário de governação, baseado em vigilância massiva e tecnologias avançadas de recolha e análise de dados, o que lhe confere uma elevada eficácia na antecipação de comportamentos desviantes, mas também

levanta sérias preocupações éticas e jurídicas.

Os resultados evidenciam que a transposição direta do DLP tal como implementado na RPC é amplamente considerada inviável, sendo esta posição sustentada por 90% dos entrevistados. As razões invocadas apontam para incompatibilidades estruturais profundas, destacando a diferença entre regimes políticos, a proteção dos direitos fundamentais e a cultura jurídica portuguesa e europeia. Embora exista um consenso quanto à impossibilidade de replicar o modelo na sua essência, a análise revelou também a existência de um espaço limitado para a incorporação seletiva de elementos tecnológicos do DLP, desde que submetidos a rigorosas salvaguardas legais e democráticas e à aprendizagem com modelos semelhantes.

Outro aspeto pertinente prende-se com a comparação entre os sistemas de videovigilância da RPC e de Portugal, onde se verificou unanimidade sobre as diferenças estruturais que os separam. Enquanto na RPC a videovigilância é um instrumento integrado de controlo social, em Portugal prevalece um modelo limitado e fortemente regulamentado, refletindo os princípios do Estado de Direito.

Outra questão abordada foi a abordagem ao DLP como um mecanismo de controlo social, imposto de forma vertical pelas instâncias superiores do poder político, nomeadamente pelo PCC, enquanto na realidade portuguesa qualquer proposta semelhante estaria necessariamente sujeita a um processo de aprovação social e validação democrática. A sua adoção dependeria de uma base legal sólida, do respeito pelas garantias constitucionais e da adesão dos cidadãos a um modelo que, mais do que controlar, fosse orientado para servir a segurança coletiva sem comprometer os direitos fundamentais.

Ao concluir esta investigação, importa sublinhar uma diferença estrutural entre o DLP tal como é aplicado na RPC e a sua eventual aplicação em Portugal. Essa diferença reside na finalidade e nos pressupostos democráticos de cada contexto. Na RPC, o DLP assume-se como um instrumento de controlo social, imposto verticalmente pelas estruturas do poder, em particular pelo PCC. Em contraste, em Portugal, qualquer implementação de um modelo semelhante exigiria aprovação social e legitimidade democrática, sendo condicionada por normas constitucionais, salvaguardas legais e respeito pelos direitos fundamentais. Assim, o que na RPC é um modelo imposto, em Portugal só poderia existir como uma escolha coletiva sustentada por valores democráticos.

Assim, este estudo reforça a importância de se pensar em políticas públicas que saibam integrar inovação tecnológica com respeito intransigente pelos direitos fundamentais, reconhecendo que a eficácia policial não pode ser alcançada à custa da

liberdade individual. A adoção parcial e cuidadosamente regulamentada de ferramentas tecnológicas inspiradas no DLP poderá representar um caminho promissor para reforçar a segurança interna em Portugal, sobretudo em áreas de maior risco, como o combate ao terrorismo e à cibercriminalidade. Contudo, qualquer evolução nesta matéria deverá ser acompanhada de um debate público, de auditorias independentes e de um reforço das capacidades institucionais, assegurando que as soluções implementadas correspondam verdadeiramente aos valores democráticos que caracterizam o sistema português. Acresce ainda que este processo de adaptação tecnológica deverá ser concebido não apenas como uma simples transposição de ferramentas digitais, mas como uma oportunidade para repensar modelos operacionais de segurança que valorizem a transparência, a participação pública e a confiança social, elementos essenciais para garantir um equilíbrio justo entre inovação e direitos fundamentais.

Esta investigação contribuiu desta forma, não só para aprofundar o conhecimento sobre a aplicabilidade de modelos tecnológicos de policiamento em contextos democráticos, oferecendo uma reflexão crítica que pode apoiar futuras decisões estratégicas, mas também para analisar o DLP em contextos autoritários como um elemento de prevenção criminal e controlo social e político.

Como limitações do estudo, destaca-se a impossibilidade de aceder a dados operacionais completos da RPC, o que condicionou parcialmente a análise. Além disso, embora o número de entrevistas tenha sido adequado ao desenho metodológico, e se tenha efetuado diversos contactos, a própria abordagem a um tema sensível aparenta demonstrar certas reservas por parte de alguns membros e instituições. Seria enriquecedor, em investigações futuras, ampliar o leque de participantes, incluindo mais profissionais de áreas técnicas e representantes da sociedade civil.

Este Trabalho de Investigação Aplicada reforça a ideia de que, embora a tecnologia possa ser um instrumento valioso na segurança interna, a sua aplicação deve sempre estar subordinada aos princípios democráticos e à proteção rigorosa dos direitos e liberdades fundamentais.

RECOMENDAÇÕES

No plano das recomendações práticas, destaca-se a pertinência de uma integração seletiva e altamente regulamentada de tecnologias como o reconhecimento facial e a análise preditiva em áreas especialmente sensíveis, nomeadamente na prevenção e combate à cibercriminalidade e ao terrorismo.

Estas aplicações devem ser sempre acompanhadas por mecanismos rigorosos de supervisão judicial e controlo democrático, assegurando que a inovação tecnológica nunca se sobreponha aos princípios da proporcionalidade e da legalidade. Paralelamente, recomenda-se o desenvolvimento de programas de formação contínua e especializada para os profissionais das forças de segurança, de modo a capacitá-los para um uso eficaz, seguro e ético destas tecnologias. Considera-se importante aprofundar o estudo da aplicação de modelos europeus de policiamento orientado por dados, na medida da tentativa de uma aproximação do DLP à realidade ocidental, privilegiando a adaptação de boas práticas que conciliem inovação tecnológica com a proteção robusta dos direitos e liberdades individuais.

Para novas linhas de estudo que permitam consolidar e expandir o conhecimento sobre esta temática, propõe-se, como prioridade, a realização de investigações que explorem a perceção pública relativamente ao uso de tecnologias de vigilância, permitindo aferir os níveis de aceitação social e as preocupações éticas que a implementação destas ferramentas suscita.

Sugere-se também a análise de projetos que implementem parcialmente instrumentos de DLP em contextos específicos, como zonas urbanas de alta densidade ou grandes eventos, com o objetivo de avaliar os impactos operacionais concretos e os riscos associados.

Outra vertente de investigação relevante passa pelo estudo aprofundado da cooperação entre entidades públicas e privadas na gestão de dados para fins de segurança, pretendendo identificar não só os benefícios e desafios regulatórios, mas também os limites necessários para preservar a confiança pública.

Estas recomendações visam não só consolidar as aprendizagens resultantes deste estudo, mas também orientar futuros esforços de reflexão e intervenção, contribuindo para a construção de uma política de segurança interna que seja simultaneamente eficaz, ética e juridicamente sólida.

REFERÊNCIAS BIBLIOGRÁFICAS

Academia Militar [AM]. (2024). NEP n.o 522/2ª/24JUN24/AM: Normas para a Redação Trabalhos Finais Investigação. Lisboa: Academia Militar.

Academia Militar [AM]. (2024). NEP nº 520/6ª/24JUN24/AM: Trabalho Final de Investigação. Lisboa: Academia Militar.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, 22(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Almeida, P. (2019). Ponto Único de Contacto para a Cooperação Policial Internacional - o Novo Paradigma. NOVA.

Al-Muntada Al-Islami Trust. (2024). Step-by-Step Hajj Guide. AWF - Al-Muntada Welfare Foundation.

Alves, C. (2008). Em busca de uma Sociologia de Polícia. Lisboa: Edição da Guarda Nacional Republicana.

Andrade, T. V. (2022). O Uso da Inteligência Artificial no Policiamento Preditivo.

Andresen, M. A., & Jenion, G. W. (2008). Crime prevention and the science of where people are. Criminal Justice Policy https://doi.org/10.1177/0887403407311591 Review, 19(2), 164–180.

Babuta, A. (2017). Big Data and Policing an Assessment of Law Enforcement Requirements, Expectations and Priorities. Royal United Services Institute.

Backer, Larry. (2019). China's Social Credit System: Data-Driven Governance for a 'New Era.' Current History. 118. 209-214. 10.1525/curh.2019.118.809.209.

Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body subject. Body & Society, 22(2), 58–81

Bao, Y. (2020). The Soft Governance of Xinjiang: The “Fanghuiju” Campaign and Surveillance in Everyday Life. Journal of the International Chinese Sociological Association, 3(1), 23–49.

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

Beraja, M., Kao, A., Yang, D. Y., & Yuchtman, N. (2021). AI-tocracy. https://doi.org/10.3386/w29466

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

Braga, A. A., Weisburd, D., & Turchan, B. (2019). Focused deterrence strategies effects on crime: A systematic review. Campbell Systematic Reviews, 15(3). https://doi.org/10.1002/cl2.1051

Brayne, S. (2017). Big data surveillance: the case of policing. American Sociological Review, 82(5), 977–1008. https://doi.org/10.1177/0003122417725865

Caprotti, F., & Liu, D. (2022). Platform urbanism and the Chinese smart city: the co-production and territorialisation of Hangzhou City Brain. GeoJournal, 87(3), 1559–1573. https://doi.org/10.1007/s10708-020-10320-2

Casolari, F., Buttaboni, C., & Floridi, L. (2023). The EU Data Act in Context: A Legal Assessment. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4584781

Cath, C. (2018). Governing artificial intelligence: ethical, legal, and technical opportunities and challenges. Philosophical Transactions of the Royal Society A, 376(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

Chan, J., & Moses, L. (2015). Is Big Data challenging criminology? Theoretical Criminology, 20(1), 21–39.

Chin, J., Lin, L. (2023). Estado de Vigilância. Relógio d' Água.

Clarke, R. (1983). Situational crime prevention: Its theoretical basis and practical scope. Crime and Justice, Vo. 4, 225-256. Consultado em http://www.jstor.org.

Clarke, R. (1997). Situational crime prevention: Successful case studies (2nd ed.). New York, USA: Harrow and Heston Publishers.

Creemers, R. (2018). "China's Social Credit System: An Evolving Practice of Control." http://dx.doi.org/10.2139/ssrn.3175792.

Cusson, M. (2007). De l'action de sécurité. In Traité de Sécurité Intérieure, Maurice Cusson, Benoît Dupon e Frédéric Lemieux (Ed.). Les Cahiers du Québec Collection Droit et Criminologie, Montréal: Éditions Hurtubise HMH.

Da Silva, L. A. M. (2009). Polícia e segurança pública no Rio de Janeiro de hoje: Uma tomada de posição. Olhares sobre a prevenção à criminalidade. Instituto ELO: Belo Horizonte.

Dakalbab, F., Talib, M. A., Waraga, O. A., Nassif, A. B., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. Social Sciences & Humanities Open, 6(1), 100342. https://doi.org/10.1016/j.ssaho.2022.100342

David, M. (2014). Modelo Integrado de Policiamento de Proximidade: Funcionalidades, Problemas e Potencialidades. ISPCI.

DCM. (2025). Portugal Data Centers. Datacentermap.com. https://www.datacentermap.com/portugal/

De Araújo, V. S., Araujo, J. J., & De Albuquerque, L. F. (2023). Policiamento preditivo na era da vigilância: a busca de um modelo constitucional e democrático. Rev. Quaestio Iuris. Rio de Janeiro Vol. 16 N.01.

De Oliveira Neiva, L. C. (2019). Big Data na investigação criminal: previsão do risco, vigilância e expectativas sociais na União Europeia. https://repositorium.sdum.uminho.pt/bitstream/1822/61235/1/3_Dissertacao_LauraNeiva.pdf

Dubois de Prisque, E. (2020). O sistema de crédito social chinês - Como Pequim avalia, recompensa e pune a sua população (Dorothéé de Bruchard, Trans.). www.fundacaofhc.org.br

Egbert S (2019) Predictive Policing and the Platformization of Police Work. Surveillance & Society 17(1/2): 83–88. DOI: 10.24908/ss.v17i1/2.12920

Fontes, Catarina, et al. (2022). AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them.Technology in Society, vol. 71. https://doi.org/10.1016/j.techsoc.2022.102137.

Fortin, M.-F. (2009). Fundamentos e etapas do processo de investigação. Loures: Lusodidacta.

Gilling, D. (1997). Crime prevention: Theory, policy and politics. London, United Kingdom: Routledge Taylor & Francis Group.

Goldstein, H., & Winners, A. (2001). Excellence in Problem-Oriented Policing. New York: Police Executive Research Forum.

Gonçalves, M. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. Information & Communications Technology Law, 26(2), 90-115.

Gonul, H. Z., & Rogenhofer, J. M. (2017). Wahhabism with Chinese Characteristics (Asia Focus #51). French Institute for International and Strategic Affairs (IRIS). https://www.iris-france.org

Grossman, Derek & Curriden, Christian & Ma, Logan & Polley, Lindsey & Williams, J.D. & Cooper, Cortez. (2020). Chinese Views of Big Data Analytics. 10.7249/RRA176-1.

Guerra, I. (2006). Pesquisa qualitativa e análise de conteúdo: Sentidos e formas de uso. Estoril: Princípia

Halford, S., & Savage, M. (2017). Speaking sociologically with big data: symphonic social science and the future for big data research. Sociology, 51(6), 1132-1148.

http://dx.doi.org/10.34620/eduser.v2i2.24

Haro, F. A., Serafim, J., Cobra, J., Faria, L., Roque, M. I., Ramos, M., Carvalho, P., & Costa, R. (2016). Investigação em Ciências Sociais - Guia Prático do Estudante. PACTOR.

Hasan, H. (2022). A Review of Hash Function Types and their Applications. Wasit Journal of Computer and Mathematics Science. 1. 120-139. 10.31185/wjcm.52.

Hu, R. (2019). The State of Smart Cities in China: The Case of Shenzhen. Energies, 12(22), 4375. https://doi.org/10.3390/en12224375

Human Right Watch. (2019). China's algorithms of repression: reverse engineering a Xinjiang police mass surveillance app. Human Rights Watch.

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. Defense and Security Analysis, 40(2), 235–269. https://doi.org/10.1080/14751798.2024.2321736

Institute for Economics & Peace. (2021) Global Peace Index 2020: Measuring Peace in a Complex World, Sydney, Junho 2020. http://visionofhumanity.org/reports

Institute for Economics & Peace. (2022) Global Peace Index 2021: Measuring Peace in a Complex World, Sydney, Junho 2021. http://visionofhumanity.org/reports

Institute for Economics & Peace. (2023) Global Peace Index 2022: Measuring Peace in a Complex World, Sydney, Junho 2022. http://visionofhumanity.org/reports

Institute for Economics & Peace. (2024) Global Peace Index 2023: Measuring Peace in a Complex World, Sydney, Junho 2023. http://visionofhumanity.org/reports

Institute for Economics & Peace. (2024). Safety Perceptions Index 2023: Understanding the impact of risk around the world.

Institute for Economics & Peace. (2025) Global Peace Index 2024: Measuring Peace in a Complex World, Sydney, Junho 2024. http://visionofhumanity.org/reports

Institute for Economics and Peace. (2024). Safety Perceptions Index 2023.

Jansen, F. (2018). Data Driven Policing in the Context of Europe. Department of Journalism, Media and Culture. Cardiff University.

Jansen, F. (2022). Data-Driven Policing: Negotiating the Legitimacy of the Police. Department of Journalism, Media and Culture. Cardiff University.

Ji, Y. (2021). The Making of Chinese Criminal Law – The Preventive Shift in the Context of the Eighth Amendment. Yuwen Li, Erasmus University Rotterdam, The Netherlands and Fu Hualing, University of Hong Kong, Hong Kong.

Kappeler, V. E. (2015). Community Policing: A Contemporary Perspective (7.ª ed.). Routledge.

Karpa, D. F., Klarl, T., & Rochlitz, M. (2022). Artificial Intelligence, Surveillance, and BigData. Springer eBooks, 145–172. https://doi.org/10.1007/978-3-031-04063-4_8

Kearns, I., Muir, Rick. (2019). Data-driven policing and public value data-driven policing and public value. The Police Foundation.

Khalfa, R., & Hardyns, W. (2023). 'Led by intelligence': A scoping review on the experimental evaluation of intelligence-led policing. Evaluation Review.

Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J., & Deibert, R. (2020). WECHAT, They Watch - How international users unwittingly build up WeChat's Chinese censorship apparatus. https://citizenlab.ca/2020/05/we-chat-they-

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. New Media and Society, 21(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Leibold, J. (2019). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. Journal of Contemporary China. 29(121), 46–60. https://doi.org/10.1080/10670564.2019.1621529

Li, Y., Barthelemy, J., Sun, S., Perez, P., & Moran, B. (2020). A Case Study of Wi-Fi Sniffing Performance Evaluation. IEEE, 8, 129224–129235. https://doi.org/10.1109/ACCESS.2020.3008533

Liang, Fan, & Chen, Y. (2022) "The Making of "Good" Citizens: China's Social Credit Systems and Infrastructures of Social Quantification." Policy & Internet, vol. 14, no. 1, pp. 114–135, https://doi.org/10.1002/poi3.291.

Liao, T., & Hwang, W. (2022). Political protests and the diversionary use of media: Evidence from China. International Interactions, 48(5), 1027–1055. doi:10.1080/03050629.2022.206527

Llinares, F. M. (2020). Predictive policing: Utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement. https://doi.org/10.31235/osf.io/a7juk

Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Lupton, D., & Michael, M. (2017). 'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance. Surveillance & Society, 15(2), 254- 268.

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

Machado, N. (2019). Big Data – paradigma tecnológico que facilita a produção de (des)igualdades. In J. Magalhães & P. Ferreira (Eds.), Livro de Atas do 5.º Congresso de Comunicação e Jornalismo (pp. 226–243). Universidade do Minho. https://repositorium.sdum.uminho.pt/handle/1822/63034

Marciniak, D. (2021). Data-Driven Policing: How Digital Technologies Transform the Practice and Governance of Policing. University of Essex.

Marilyn Peterson. (2005). Intelligence-Led Policing: The New Intelligence Architecture. www.ojp.usdoj.gov/BJA

Marsal-Llacuna, Maria-Lluïsa, Colomer-Llinàs, Joan and Meléndez-Frigola, Joaquim, (2015), Lessons in urban monitoring taken from sustainable and livable cities to better

address the Smart Cities initiative, Technological Forecasting and Social Change, 90, issue PB, p. 611-622.

Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. International Journal of Public Administration, 42(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Melo, P. V., & Viseu, A. (2024). 20 anos de videovigilância dos espaços públicos em Portugal: panorama e desafios sociopolíticos. https://orcid.org/0000-0001-5450-2338

Oliveira, J. F. de (2006). As políticas de segurança e os modelos de policiamento: A emergência do policiamento de proximidade. Coimbra: Almedina.

Organization for Security and Co-operation in Europe. (2017). The OSCE Project on Project Report. OSCE.

Oswald M., Urwin, S. (2017). Algorithms in Policing: Take Algo-Care™: Written evidence. University of Winchester

Pinheiro, P. (2014). Adoção de Sistemas Cloud Computing.

Piza, E. L. (2024, julho). I studied ShotSpotter in Chicago and Kansas City – Here's What People in Detroit and the More Than 167 Other Cities and Towns Using This Technology Should Know. National Institute of Justice.

Purves, D., Davis, J., & Gilbert, J. (2022). 5 Challenges Facing Data-Driven Policing,

Quivy, R., & Campenhoudt, L. V. (2019). Manual de investigação em ciências sociais (7.ª ed.). Lisboa: Gradiva.

Ratcliffe, J. H. (2016). Intelligence-led policing. Routledge.

Richards, N., King, J. (2014). Big Data Ethics. Wake Forest Law Review. Vol. 49.

Rodrigues, C. B. (2019). Segurança Pública: Modelos de Policiamento. Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

Saheb, T. (2023). "Ethically contentious aspects of artificial intelligence surveillance: a

social science perspective". AI and Ethics. https://doi.org/10.1007/s43681-022-00196-y

Sampaio, J. (2021). Das teorias à prevenção criminal (estudo sobre a conexão e prevenção do crime tendo em conta os espaços urbanos e a estrutura social). ISMAI.

Sarmento, M. (2013). Metodologia científica para a elaboração, escrita e apresentação de teses (Vol. 1). Universidade Lusíada.

Sentou-se, J. (2011). Prevenção ao crime e teoria social. Novas e antigas questões. Lua Nova: Revista de cultura e política. Ed. 83. Unicamp: São Paulo.

Shalev-Shwartz, S., & Ben-David, S. (2014). Understanding Machine Learning: From Theory to Algorithms. http://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning

Sprick, D. (2020). 'Killing Rats in the Street' for the paramount human right of security: The law and policy of China's People's War on Terror. In Martin Scheinin, Christophe Paulusson (eds.). Human dignity and human security in times of terrorism. Den Haag: Asser Press: 181-205

SSI. (2024). Relatório Anual de Segurança Interna 2023. XXI Governo Constitucional.

Tiwari, S. (2022). The Reality of Cyber Operations in The Grey Zone– The Emerging Geopolitics, The Defense Horizon Journal.

Torres, J. E. M. (2015). Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança. Lisboa: ISCPSI.

Tribunal de Contas Europeu. (2023). Relatório Especial - Cidades inteligentes: Soluções concretas, mas fragmentação é obstáculo à difusão. doi: 10.2865/223600

Tu, F. (2016). WeChat and civil society in China. Communication and the Public, 1(3), 343–350. https://doi.org/10.1177/2057047316667518

UUK. (2025). Evidence to the Science, Innovation and Technology Committee inquiry on innovation, growth and the regions. Londres

Wang, M. (2019). China's algorithms of repression: reverse engineering a Xinjiang police mass surveillance app (Human Right Watch, Ed.). Human Rights Watch.

World Justice Project. (2023). WJP Rule of Law Index. Worldjusticeproject.org. https://worldjusticeproject.org/rule-of-law-index/

Wu, Y., Sun, I. Y., & Hu, R. (2021). Cooperation with police in China: Surveillance cameras, neighborhood efficacy, and policing. Social Science Quarterly, 102(1), 433–451. https://doi.org/10.1111/ssqu.12903

Xi Jinping (习近平). 2016. Perfecting the socialist social governance system with Chinese characteristics. Tireless working on an increasing level of a safe China.

Xiaolin, Duan. (2024). "Domestic Sources of China's Wolf-Warrior Diplomacy: Individual Incentive, Institutional Changes and Diversionary Strategies." The Pacific Review, vol. 37, no. 3, pp. 585–603, https://doi.org/10.1080/09512748.2023.2205163.

Yang, D. Y. (2024). China: Autocracy 2.0 (NBER Working Paper No. 32993). National Bureau of Economic Research. http://www.nber.org/papers/w32993

Yaseen, H. K., & Obaid, A. M. (2020). Big data: Definition, architecture & applications. International Journal on Informatics Visualization, 4(1), 45–51.

Zhu et al. (2024). How different can smart cities be? A typology of smart cities in China. Cities. DOI:10.1016/j.cities.2024.104992

Zygiaris, S. (2012). Smart City Reference Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems. Journal of the Knowledge Economy, 4(2), 217–231. https://doi.org/10.1007/s13132-012-0089-4

REFERÊNCIAS BIBLIOGRÁFICAS LEGAIS

Conselho da União Europeia (2009). Decisão 2009/902/JAI do Conselho: criação de uma Rede Europeia de Prevenção da Criminalidade. Jornal Oficial da União Europeia, L 321 de 8.12.2009, pp. 44-46.

Decisão 15809/18, do Concelho da União Europeia (2018). Estabelece uma recomendação para suprir as deficiências identificadas na avaliação de 2017 da aplicação pela República Portuguesa do acervo de Schengen no domínio da cooperação policial. Bruxelas.

Decreto-lei n.º 10/2020, de 11 de março. (2020). Estabelece a orgânica do Ponto Único de Contacto para a Cooperação Policial Internacional. Diário da República n.º 50/2020, Série I, 2-6. Lisboa: Presidência do Conselho de Ministros.

Lei n.º 49/2008, de 27 de agosto da Assembleia da República. (2008). Diário da República n.º 165/2008, Série I de 2008-08-27. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-67191210-67192945

Lei n.º 49/2008, de 27 de agosto. (2008). Aprova a Lei de Organização da Investigação Criminal. Diário da República n.º 165/2008, Série I, 6038 - 6042. Lisboa: Assembleia da República.

Lei n.º 51/2023, de 28 de agosto da Assembleia da República. (2023). Diário da República n.º 167/2020, Série I de 2020-08-27, páginas 2 – 11. https://diariodarepublica.pt/dr/detalhe/lei/55-2020-141259621

Lei n.º 53/2008, de 29 de agosto. (2008). Aprova a Lei de Segurança Interna. Diário da República n.º 167/2008, Série I, 6135 - 6141. Lisboa: Assembleia da República

Lei n.º 63/2007, de 06 de novembro da Assembleia da República. (2007). Diário da República n.º 213/2007, Série I de 2007-11-06. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2007-107794647-107802525

Lei n.º 73/2009, de 12 de agosto. (2009). Estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos órgãos

de polícia criminal. Diário da República n.º 155/2009, Série I, 5217 - 5220. Lisboa: Assembleia da República

Lei n.º 95/2021, de 29 de dezembro. (2021). Regula a utilização e o acesso a sistemas de videovigilância. Diário da República n.º 218/2021, Série I de 2021-11-10. Lisboa: Assembleia da República.

National People's Congress of China. (2020). Criminal Law of the People's Republic of China. http://www.npc.gov.cn

National People's Congress of China. (2015). National Security Law of the People's Republic of China. http://www.npc.gov.cn

National People's Congress of China. (2021). Personal Information Protection Law of the People's Republic of China (PIPL). http://www.npc.gov.cn

Regulamento n.º 679/2016, de 27 de abril. (2016). Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (EU). Jornal Oficial da União Europeia. Bruxelas

APÊNDICES

Apêndice A – Tabela de relação de autor, referência bibliográfica, revista e quartil.

Autor(es)	Referência	Revista	Quartil
Albino, V., Berardi, U., & Dangelico, R. M.	(Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, 22(1), 3–21. https://doi.org/10.1080/10630732.2014.942092	Journal of Urban Technology	Q1
Andresen, M. A., & Jenion, G. W.	(Andresen, M. A., & Jenion, G. W. (2008). Crime prevention and the science of where people are. Criminal Justice Policy https://doi.org/10.1177/0887403407311591 Review, 19(2), 164–180.	Criminal Justice Policy Review	Q2
Babuta, A.	Babuta, A. (2017). Big Data and Policing an Assessment of Law Enforcement Requirements, Expectations and Priorities. Royal United Services Institute.	Royal United Services Institute	Q1
Ball, K., Di Domenico, M., & Nunan, D.	Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body subject. Body & Society, 22(2), 58–81	Body & Society	Q1
Bartlett, A., Lewis, J., Reyes-Galindo, L., & Stephens, N.	Bartlett, A., Lewis, J., Reyes-Galindo, L., & Stephens, N. (2018). The locus of legitimate interpretation in Big Data sciences: Lessons for computational social science from-omic biology and high-energy physics. Big Data & Society, 5(1), 1-15.	Big Data & Society	Q1
Braga, A. A., Weisburd, D., &	Braga, A. A., Weisburd, D., & Turchan, B. (2019). Focused deterrence strategies effects on crime: A systematic review. Campbell Systematic Reviews, 15(3). https://doi.org/10.1002/cl2.1051	Campbell Systematic Reviews	Q2

Turchan, B.			
Brayne, S.	Brayne, S. (2017). Big data surveillance: the case of policing. American Sociological Review, 82(5), 977–1008. https://doi.org/10.1177/0003122417725865	American Sociological Review	Q1
Caprotti, F., & Liu, D.	Caprotti, F., & Liu, D. (2022). Platform urbanism and the Chinese smart city: the co-production and territorialisation of Hangzhou City Brain. GeoJournal, 87(3), 1559–1573. https://doi.org/10.1007/s10708-020-10320-2	GeoJournal	Q2
Casolari, F., Buttaboni, C., & Floridi, L.	Casolari, F., Buttaboni, C., & Floridi, L. (2023). The EU Data Act in Context: A Legal Assessment. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4584781	SSRN Electronic Journal	Q1
Cath, C.	Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. Philosophical Transactions of the Royal Society A, 376(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080	Philosophical Transactions of the Royal Society A	Q1
Chan, J., & Moses, L.	Chan, J., & Moses, L. (2015). Is Big Data challenging criminology? Theoretical Criminology, 20(1), 21–39.	Theoretical Criminology	Q1
Dakalbab, F., et al.	Dakalbab, F., Talib, M. A., Waraga, O. A., Nassif, A. B., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. Social Sciences & Humanities Open, 6(1), 100342. https://doi.org/10.1016/j.ssaho.2022.100342	Social Sciences & Humanities Open	Q1
De Araújo,	De Araújo, V. S., Araujo, J. J., & De	Rev. Quaestio	Q1

V. S., et al.	Albuquerque, L. F. (2023). Policiamento preditivo na era da vigilância: a busca de um modelo constitucional e democrático. Rev. Quaestio Iuris. Rio de Janeiro Vol. 16 N.01.	Iuris	
Egbert, S.	Egbert S (2019) Predictive Policing and the Platformization of Police Work. Surveillance & Society 17(1/2): 83–88. DOI: 10.24908/ss. v17i1/2.12920	Surveillance & Society	Q2
Fontes, C., et al.	Fontes, Catarina, et al. (2022). AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them.Technology in Society, vol. 71. https://doi.org/10.1016/j.techsoc.2022.102137.	Technology in Society	Q1
Gonçalves, M.	Gonçalves, M. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. Information & Communications Technology Law, 26(2), 90-115.	Information & Communications Technology Law	Q1
Halford, S., & Savage, M.	Halford, S., & Savage, M. (2017). Speaking sociologically with big data: symphonic social science and the future for big data research. Sociology, 51(6), 1132-1148. http://dx.doi.org/10.34620/eduser.v2i2.24	Sociology	Q1
Hasan, H.	Hasan, H. (2022). A Review of Hash Function Types and their Applications. Wasit Journal of Computer and Mathematics Science. 1. 120-139. 10.31185/wjcm.52.	Wasit Journal of Computer and Mathematics Science	Q1
Hu, R.	Hu, R. (2019). The State of Smart Cities in China: The Case of Shenzhen. Energies, 12(22), 4375. https://doi.org/10.3390/en12224375	Energies	Q1
Hunter, L. Y., et al.	Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major	Defense and Security Analysis	Q2

	power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. Defense and Security Analysis, 40(2), 235–269. https://doi.org/10.1080/14751798.2024.2321736		
Jansen, F.	Jansen, F. (2018). Data Driven Policing in the Context of Europe. Department of Journalism, Media and Culture. Cardiff University.	Department of Journalism, Media and Culture, Cardiff University	Q1
Jansen, F.	Jansen, F. (2022). Data-Driven Policing: Negotiating the Legitimacy of the Police. Department of Journalism, Media and Culture. Cardiff University.	Department of Journalism, Media and Culture, Cardiff University	Q1
Karpa, D. F., Klarl, T., & Rochlitz, M.	Karpa, D. F., Klarl, T., & Rochlitz, M. (2022). Artificial Intelligence, Surveillance, and BigData. Springer eBooks, 145–172. https://doi.org/10.1007/978-3-031-04063-4_8	Springer eBooks	Q1
Khalfa, R., & Hardyns, W.	Khalfa, R., & Hardyns, W. (2023). 'Led by intelligence': A scoping review on the experimental evaluation of intelligence-led policing. Evaluation Review.	Evaluation Review	Q2
Leibold, J.	Leibold, J. (2019). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. Journal of Contemporary China. 29(121), 46–60. https://doi.org/10.1080/10670564.2019.1621529	Journal of Contemporary China	Q1
Li, Y., et al.	Li, Y., Barthelemy, J., Sun, S., Perez, P., & Moran, B. (2020). A Case Study of Wi-Fi Sniffing Performance Evaluation. IEEE, 8, 129224–129235.	IEEE	Q1

	https://doi.org/10.1109/ACCESS.2020.3008533		
Liang, F., & Chen, Y.	Liang, Fan, and Yuchen Chen. (2022) "The Making of "Good" Citizens: China's Social Credit Systems and Infrastructures of Social Quantification." Policy & Internet, vol. 14, no. 1, pp. 114–135, https://doi.org/10.1002/poi3.291.	Policy & Internet	Q1
Liao, T., & Hwang, W.	Liao, T., & Hwang, W. (2022). Political protests and the diversionary use of media: Evidence from China. International Interactions, 48(5), 1027–1055. doi:10.1080/0 3050629.2022.206527	International Interactions	Q2
Lum, K., & Isaac, W.	Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x	Significance	Q2
Lupton, D., & Michael, M.	Lupton, D., & Michael, M. (2017). 'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance. Surveillance & Society, 15(2), 254- 268.	Surveillance & Society	Q2
Lyon, D.	Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, 1(2). https://doi.org/10.1177/2053951714541861	Big Data & Society	Q1
Meijer, A., & Wessels, M.	Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. International Journal of Public Administration, 42(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664	International Journal of Public Administration	Q2
Saheb, T.	Saheb, T. (2023). "Ethically contentious aspects of artificial intelligence surveillance: a social science perspective". AI and Ethics. https://doi.org/10.1007/s43681-022-00196-y	AI and Ethics	Q2
Wu, Y., Sun,	Wu, Y., Sun, I. Y., & Hu, R. (2021). Cooperation with police in China: Surveillance	Social Science Quarterly	Q2

I. Y., & Hu, R.	cameras, neighborhood efficacy, and policing. Social Science Quarterly, 102(1), 433–451. https://doi.org/10.1111/ssqu.12903		
Xiaolin, Duan	Xiaolin, Duan. (2024). "Domestic Sources of China's Wolf-Warrior Diplomacy: Individual Incentive, Institutional Changes and Diversionary Strategies." The Pacific Review, vol. 37, no. 3, pp. 585–603, https://doi.org/10.1080/09512748.2023.2205163.	The Pacific Review	Q1
Zhu et al.	Zhu et al. (2024). How different can smart cities be? A typology of smart cities in China. Cities. DOI: 10.1016/j.cities.2024.104992	Cities	Q1
Zygiaris, S.	Zygiaris, S. (2012). Smart City Reference Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems. Journal of the Knowledge Economy, 4(2), 217–231. https://doi.org/10.1007/s13132-012-0089-4	Journal of the Knowledge Economy	Q1

Apêndice B - Guião da Entrevista

Guião de Entrevista

ACADEMIA MILITAR
DIRECÇÃO DE ENSINO

Mestrado Integrado em Ciências Militares, na Especialidade de Segurança (GNR)

TRABALHO DE INVESTIGAÇÃO APLICADA

A utilização do *Data Led Policing* na prevenção criminal: Estudo de caso da República Popular da China

AUTOR: Aspirante GNR Cavalaria Miguel Jacob Sena Sardinha
ORIENTADOR: Major de Infantaria da GNR Adriana Martins

Lisboa, 18 de março de 2025

Carta de Apresentação

A presente Entrevista faz parte integrante da realização do Trabalho de Investigação Aplicada (TIA) para a conclusão do mestrado Integrado em Ciências Militares, na especialidade Segurança. O TIA subordinado ao tema *"A utilização do Data Led Policing na prevenção criminal: Estudo de caso da República Popular da China"* tem como objetivo analisar as estratégias do Data Led Policing utilizadas na RPC para a prevenção criminal, analisar o impacto do Data Led Policing na redução da criminalidade e analisar a aplicabilidade do Data Led Policing em Portugal.

O Data Led Policing é uma abordagem ao policiamento que retira partido dos Big Data para aumentar a vigilância. Tem como principais atributos a "recolha e tratamento de dados pessoais incluindo, em tempo real, empregando sistemas automatizados e monitorizadores de rotinas e a identificação, seguimento, regulação, previsão, prescrição, prevenção e orientação de comportamentos de indivíduos ou grupos" (Jansen, 2022, p. 2).

No âmbito desta investigação, a análise das estratégias do Data Led Policing na República Popular da China é fundamental para compreender a sua relação com a prevenção criminal, num contexto com características próprias. Não obstante, a investigação procura compreender a possibilidade da aplicação do Data Led Policing em Portugal, tendo por base a sua aplicação na República Popular da China.

Com o propósito de obter informações relevantes e válidas relativamente às matérias supracitadas, solicito a Vossa Excelência que me conceda uma entrevista sobre o tema em apreço, tendo em conta que o seu contributo é fundamental para atingir os objetivos propostos para a presente investigação.

Grato desde já pela sua disponibilidade e atenção.

Atenciosamente,

Miguel Jacob Sena Sardinha
Aspirante de Cavalaria da Guarda Nacional Republicana

PROTOCOLO DE CONSENTIMENTO INFORMADO

O presente protocolo é estabelecido entre Miguel Jacob Sena Sardinha, aluno da AM a realizar investigação com o tema: *"A utilização do Data Led Policing na prevenção criminal: Estudo de caso da República Popular da China"*, e o participante: _____,
através do método de entrevista.

O investigador e o orientador científico comprometem-se a:

a) Conduzir a investigação de acordo com os parâmetros de qualidade preconizados pela comunidade científica da especialidade;

b) Discutir e negociar outros aspetos específicos de cada caso relativos à confidencialidade da informação, se solicitado pelo participante;

c) Impedir qualquer divulgação de informação referente aos participantes, exteriormente à equipa de investigação, sem o consentimento prévio de todos os envolvidos;

d) Entregar uma síntese descritiva dos resultados aos participantes, através de correio eletrónico;

e) Manter os participantes a par do trabalho que está a ser desenvolvido, nomeadamente no que concerne à análise dos dados, sempre que os mesmos o solicitem;

f) Prestar aos participantes no processo todos os esclarecimentos solicitados no decorrer da investigação;

g) Cumprir o Código Deontológico da *American Psychological Associantion* (APA 7ª Edição) na realização da investigação;

h) Eliminar todas as gravações áudio após o decorrer da investigação e a defesa pública da tese.

Os participantes comprometem-se a:

a) Prestar informações sobre a sua experiência no caso em estudo e sobre a sua experiência profissional;

b) Ser entrevistado num momento acordado entre o investigador e o participante;

c) Autorizar a gravação áudio da entrevista, a pedido do investigador;

d) Decidir mencionar ou omitir a sua participação no projeto nos contextos profissionais em que considere conveniente fazê-lo;

e) Permitir a publicação do resultado do estudo, com omissão da sua identidade, nomeadamente nas seguintes situações:

I. Tese de Mestrado a apresentar à Academia Militar;
II. Comunicações em congressos científicos-profissionais;
III. Publicações científicas em revistas e/ou em livros da especialidade.

Assinaturas:

_____

(Participante)

_____

(Investigador)

Local e Data:

_____

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	Hora (Início/Fim):
U/E/O:	Data:
Função/Posto:	Local:

ENTREVISTA

As respostas irão servir única e exclusivamente como objeto de estudo para a investigação, pelo que lhe é solicitada autorização para efetuar gravação e posterior análise e transcrição das respostas. Os padrões éticos e morais serão observados. Igualmente será respeitada o princípio da confidencialidade. Após realizada a entrevista as transcrições serão remetidas ao entrevistado, para apreciação e validação, garantindo a precisão da informação recolhida.

Questão 1:

Na sua perspetiva, seria possível a aplicação do "modelo" Data Led Policing, nos modelos aplicados na República Popular da China, em Portugal?

Questão 2:

Na sua perspetiva, de que forma poderia ser adaptado o "modelo" Data Led Policing aplicado na República Popular da China em Portugal?

Questão 3:

Na sua perspetiva, de que forma é que o "modelo" Data Led Policing, adaptado às características de Portugal, poderia concorrer para garantir a segurança interna?

Questão 4:

Na sua perspetiva, o modelo de videovigilância implementado em Portugal para prevenir a criminalidade apresenta similitudes ao "modelo" Data Led Policing aplicado na República Popular da China?

Questão 5:

Na sua perspetiva, que desafios existiram na adoção do "modelo" Data Led Policing em Portugal?

Apêndice C – Tabela de análise de Entrevistas

Categoria	Subcategoria	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	%
1. Viabilidade do DLP em Portugal	1.1. Incompatibilidades Jurídicas	X	X	X	X	X	X	X	X	X	X	100
	1.2. Incompatibilidades Políticas	X	X		X	X	X	X	X	X	X	90
	1.3. Incompatibilidades Culturais	X	X	X	X	X	X		X	X	X	90
	1.4. Outras Restrições	X										10
2.Adaptação Potencial	2.1. Tecnologias Adaptáveis			X	X		X		X	X	X	60
	2.2. Limites Jurídicos	X	X	X	X	X	X	X	X	X	X	100
	2.3. Propostas Específicas (terrorismo, cibercrime)			X	X							20
	2.4. Riscos Éticos	X	X		X	X	X	X	X	X		80
3.Contributos para a Segurança Interna	3.1. Aumento de Eficiência e Eficácia		X	X	X	X	X	X	X	X	X	90
	3.2. Aumento da Sensação de Segurança						X	X	X	X	X	50
	3.3. Riscos de Vigilância Excessiva	X	.X		X	X	X	X				60
	3.4. Exigências Legais	X	X	X	X	X	X	X	X	X	X	100
4. Videovigilância	4.1. Diferenças Estruturais (Finalidade)	X	X	X	X	X	X	X	X	X	X	100
	4.2. Semelhanças Técnicas		X	X			X	X		X	X	60
	4.3. Riscos de Dependência Tecnológica						X	X	X			30
	4.4 Difícil aceitação Pública	X	X		X		X	X	X	X	X	80
5. Obstáculos	5.1. Limitações Legais	X	X	X	X	X	X	X	X	X	X	100
	5.2. Fragmentação Institucional		X	X			X	X	X		X	70
	5.3. Fatores Culturais	X		X	X	X	X	X	X	X	X	90
	5.4. Desafios Políticos	X	X	X	X	X	X	X	X	X	X	100