

Universidades Lusíada

Moreira, Carla Melissa Vaz Landim, 1997-

Da videoproteção urbana inteligente : prevenção de incivildade - caso de Lisboa

<http://hdl.handle.net/11067/7743>

Metadados

Data de Publicação	2024
Resumo	<p>A cidade apresenta-se atualmente como um denso aglomerado populacional na qual os laços de convivência são fracos, o anonimato impera e os comportamentos antissociais têm maior propensão para ocorrer. A dissociação moral e cultural entre o indivíduo e a sociedade pode gerar nalguns dos seus membros a propensão para a prática de atividades antissociais crimínógenas. Abraçando o desenvolvimento e a inovação tecnológica, a tarefa de garantir a segurança pode torna-se mais eficiente. Neste contexto...</p> <p>The city is currently a dense population agglomeration in which the bonds of coexistence are weak, anonymity reigns and antisocial behavior is more likely to occur. The moral and cultural dissociation between the individual and society can generate in some of its members a propensity to engage in criminogenic antisocial activities. By embracing technological development and innovation, the task of ensuring security can become more efficient. In this context, the video surveillance system emerge...</p>
Palavras Chave	Círculo fechado de televisão - Portugal - Lisboa, Prevenção do crime - Portugal - Lisboa, Segurança pública - Portugal - Lisboa
Tipo	masterThesis
Revisão de Pares	Não
Coleções	[ULL-FD] Dissertações

Esta página foi gerada automaticamente em 2025-01-09T06:52:13Z com informação proveniente do Repositório



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

**Da videoproteção urbana inteligente: prevenção de
incivilidade - caso de Lisboa**

Realizado por:

Carla Melissa Vaz Landim Moreira

Orientado por:

Professor Doutor Pedro José Lopes Clemente

Constituição do Júri:

Presidente: Professor Doutor José Alberto Rodríguez Lorenzo González
Orientador: Professor Doutor Pedro José Lopes Clemente
Arguente: Professor Doutor Sérgio Ricardo Costa Chagas Felgueiras

Dissertação aprovada em: 04 de dezembro de 2024

Lisboa

2024



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

Da videoproteção urbana inteligente: prevenção de incivilidade - caso de Lisboa

Carla Melissa Vaz Landim Moreira

Lisboa

Agosto 2024



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

Da videoproteção urbana inteligente: prevenção
de incivilidade - caso de Lisboa

Carla Melissa Vaz Landim Moreira

Lisboa

Agosto 2024

Carla Melissa Vaz Landim Moreira

Da videoproteção urbana inteligente: prevenção de incivilidade - caso de Lisboa

Dissertação apresentada à Faculdade de Direito da Universidade Lusíada para a obtenção do grau de Mestre em Segurança e Justiça.

Orientador:
Professor Doutor Pedro José Lopes Clemente

Lisboa

Agosto 2024

FICHA TÉCNICA

Autora Carla Melissa Vaz Landim Moreira
Orientador Professor Doutor Pedro José Lopes Clemente
Título Da videoproteção urbana inteligente: prevenção de incivilidade - caso de Lisboa
Local Lisboa
Ano 2024

CASA DO CONHECIMENTO DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

MOREIRA, Carla Melissa Vaz Landim, 1997-

Da videoproteção urbana inteligente : prevenção de incivilidade - caso de Lisboa / Carla Melissa Vaz Landim Moreira ; orientado por Pedro José Lopes Clemente. - Lisboa : [s.n.], 2024. - Dissertação de mestrado em Segurança e Justiça, Faculdade de Direito da Universidade Lusíada.

I - CLEMENTE, Pedro José Lopes, 1959-

LCSH

1. Circuito fechado de televisão - Portugal - Lisboa
 2. Prevenção do crime - Portugal - Lisboa
 3. Segurança pública - Portugal - Lisboa
 4. Universidade Lusíada. Faculdade de Direito - Teses
 5. Teses - Portugal - Lisboa
-
1. Closed-circuit television - Portugal - Lisbon
 2. Crime prevention - Portugal - Lisbon
 3. Public safety - Portugal - Lisbon
 4. Universidade Lusíada. Faculdade de Direito - Dissertations
 5. Dissertations, Academic - Portugal - Lisbon

1. HV7936.T4 M67 2024

AVISO LEGAL

O conteúdo desta dissertação reflete as perspectivas, o trabalho e as interpretações da autora no momento da sua entrega. Esta dissertação pode conter incorreções, tanto conceptuais como metodológicas, que podem ter sido identificadas em momento posterior ao da sua entrega. Por conseguinte, qualquer utilização dos seus conteúdos deve ser exercida com cautela. Ao entregar esta dissertação, a autora declara que a mesma é resultante do seu próprio trabalho, contém contributos originais e são reconhecidas todas as fontes utilizadas, encontrando-se tais fontes devidamente citadas no corpo do texto e identificadas na secção referências. A autora declara, ainda, que não divulga na presente dissertação quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor ou de propriedade industrial.

AGRADECIMENTOS

Deixo o meu sincero agradecimento ao Professor Doutor José Pedro Lopes Clemente, pela disponibilidade e prontidão de ação, pelo tempo disponibilizado para educar e guiar-me nesta caminhada, pelo humanismo com que guia.

O meu agradecimento ao Professor Doutor António Manuel Fernandes da Silva Ribeiro pela virtude que transmite através dos seus ensinamentos e pelo humanismo com que orienta os estudantes.

O meu genuíno elogio e agradecimento a todas as professoras que me inspiraram, desde o ensino primário até este momento, com especial apreço à professora Patrícia, à professora Nazaré Sebastião, à professora Carolina, à professora Helena Braga, à professora Maria Fernanda e à professora Teresa Nunes.

RESUMO

A cidade apresenta-se atualmente como um denso aglomerado populacional na qual os laços de convivência são fracos, o anonimato impera e os comportamentos antissociais têm maior propensão para ocorrer. A dissociação moral e cultural entre o indivíduo e a sociedade pode gerar nalguns dos seus membros a propensão para a prática de atividades antissociais crimínógenas.

Abraçando o desenvolvimento e a inovação tecnológica, a tarefa de garantir a segurança pode torna-se mais eficiente. Neste contexto, o sistema de videovigilância surge como instrumento de proteção que observa imparcialmente, apenas distinguindo da massa os agentes com comportamento suspeito e tendencialmente criminoso.

Dispondo do desenvolvimento tecnológico ocorrido no último século, o setor da segurança poderá aumentar a eficácia da investigação criminal assim como a prevenção criminal utilizando tanto aplicações tecnológicas como algoritmos informáticos para a deteção precoce de criminalidade e incivildades.

Conjugando o meio urbano, como local preferencial para a prática de ilícitos e incivildades, com especial destaque para a criminalidade violenta e organizada, na realidade portuguesa a cidade de Lisboa surge como objeto de experimentação relevante devido ao facto de compreender o distrito com mais criminalidade registada do território português.

A problemática em apreço expressa a oportunidade de, em nome da prevenção criminal e da segurança nacional, fazer uso da videovigilância e da Inteligência Artificial como meios de proteção da população. Examinando o essencial binómio Segurança versus Liberdade, conjuga-o com o uso da Videovigilância e da Inteligência Artificial, propomos analisar o estado da arte do uso de aplicações tecnológicas e algoritmos informáticos para a prevenção de criminalidade e incivildades.

PALAVRAS CHAVES: Videoproteção, prevenção, Inteligência Artificial, incivildades, cidade inteligente

ABSTRACT

The city is currently a dense population agglomeration in which the bonds of coexistence are weak, anonymity reigns and antisocial behavior is more likely to occur. The moral and cultural dissociation between the individual and society can generate in some of its members a propensity to engage in criminogenic antisocial activities.

By embracing technological development and innovation, the task of ensuring security can become more efficient. In this context, the video surveillance system emerges as a protection tool that observes impartially, only distinguishing agents with suspicious and tendentially criminal behavior from the mass.

With the technological development that has taken place over the last century, the security sector can increase the effectiveness of criminal investigation as well as crime prevention by using both technological applications and computer algorithms for the early detection of crime and incivilities.

Combining the urban environment as a preferential place for the practice of illicit and, incivilities with special emphasis on violent and organized crime, in the Portuguese reality the city of Lisbon emerges as a relevant experimentation object as the district with the most recorded crime in Portuguese territory.

The issue at hand expresses the opportunity, in the name of crime prevention and national security, to use video surveillance and Artificial Intelligence as a means of protecting the population. Examining the essential binomial of Security versus Freedom and combining it with the use of Video Surveillance and Artificial Intelligence, we propose to analyse the state of the art in the use of technological applications and computer algorithms for the prevention of crime and incivilities.

KEYWORDS: Video protection, prevention, Artificial Intelligence, incivilities, Smart city

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AP - Administração Pública

ANN - *Artificial Neural Networks*

ANEPC - Autoridade Nacional de Emergência e Proteção Civil

CC - Código Civil

CCTV - *Closed Circuit Television*

CPTED - *Crime Prevention Through Environmental Design*

CNPD - Comissão Nacional de Proteção de Dados

CPP - Código de Processo Penal

CRP - Constituição da República Portuguesa

DL - *Deep Learning*

HAR - *Human Action Detection*

IA - Inteligência Artificial

ML - *Machine Learning*

OR - *Odds-ratio*

RASI - Relatório Anual de Segurança Interna

RGPD - Regulamento Geral sobre a Proteção de Dados

TIC - Tecnologias de Informação e Comunicação

UE - União Europeia

1. Índice

INTRODUÇÃO.....	15
1.1. ENQUADRAMENTO	16
1.2. METODOLOGIA.....	16
1.3. ESCOLHA E JUSTIFICAÇÃO DO TEMA	16
1.4. DELIMITAÇÃO DO OBJETO DE ESTUDO: OBJETIVO GERAL.....	17
1.5. DELIMITAÇÃO DO OBJETO DE ESTUDO: OBJETIVO ESPECÍFICO	17
1.6. PERGUNTAS DE INVESTIGAÇÃO.....	17
1.7. ESTRUTURA DA DISSERTAÇÃO	18
2. NATUREZA HUMANA, SOCIEDADE, CRIME	20
2.1. DESVIO E CRIME	22
2.2. INCIVILIDADES	24
2.3. SEGURANÇA PÚBLICA.....	27
2.3.1. PREVENÇÃO CRIMINAL	32
3. VIDEOVIGILÂNCIA.....	35
3.1. INTELIGÊNCIA ARTIFICIAL	39
3.1.1. DOMÍNIOS DA INTELIGÊNCIA ARTIFICIAL: BIG DATA, MACHINE LEARNING, DEEP LEARNING.....	41
3.2. SMART CITY: RURAL VS URBANO, SMART CITY.....	42
4. ADMINISTRAÇÃO PÚBLICA	46
4.1. POLÍTICAS PÚBLICAS	47
4.2. POLÍTICAS DE SEGURANÇA	48
5. CRIMINALIDADE EM PORTUGAL	49
5.1. CRIMINALIDADE VIOLENTA.....	51
5.2. SENTIMENTO DE INSEGURANÇA	53
5.3. SEGURANÇA EM SMART CITIES.....	54
5.4. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES	57
5.4.1. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES: CRÍTICAS.....	58
5.4.2. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES: BENEFÍCIOS	62
5.5. CCTV INTELIGENTE	67
6. VULNERABILIDADES ASSOCIADAS AO SISTEMA CCTV.....	71
6.1. VULNERABILIDADES TECNOLÓGICAS.....	72
6.2. ENQUADRAMENTO LEGAL CCTV EM PORTUGAL.....	75
6.3. ENQUADRAMENTO LEGAL IA EM PORTUGAL E NA UNIÃO.....	79
7. ESTUDO DE CASO	81
8. CONCLUSÃO	85
9. BIBLIOGRAFIA	86

INTRODUÇÃO

Num cenário no qual o Homem partilha o mesmo espaço geográfico com os seus congêneres e exerce livremente os seus apetites, ocorre necessariamente que este coaja os seus semelhantes para atingir os seus fins; ou no reverso se não dispuser de meios para impor a sua vontade, sofrerá coerção por parte dos seus semelhantes. Para livrar-se da violência exercida pelos seus semelhantes e proteger os seus haveres, o Homem foi forçado a associar-se e formar comunidades políticas.

Porque para possibilitar a plena realização do potencial cognitivo e social do ser humano é necessário proteger os membros de uma sociedade dos comportamentos antissociais levados a cabo entre associados, para cumprir essa função no aparelho regulador- Estado- é delegada a tarefa de garantir a tranquilidade pública.

Quando a prática de determinados comportamentos é considerada prejudicial para a manutenção da ordem pública e para a conservação do tecido social, a coletividade determina que tais comportamentos não são toleráveis e devem ser reprovados.

A segurança é erroneamente associada à coação jurídica e material, à restrição de direitos, liberdades e garantias. A segurança não deve ser encarada exclusivamente através de uma perspetiva repressiva, que realça a sua dimensão coerciva, mas também através de uma perspetiva humanista: a segurança como bem jurídico coletivo garantístico do exercício dos direitos, liberdades e garantias.

1.1. ENQUADRAMENTO

A presente investigação surge como imperativo para a obtenção do grau de mestre em Segurança e Justiça, pela Faculdade de Direito da Universidade Lusíada de Lisboa. Enquadra-se no domínio das Ciências Humanas e Sociais, mais particularmente na área científica da Segurança. Constitui uma importante etapa na formação académica bem como uma ferramenta de melhoramento profissional. Não menos relevante, a presente investigação é um meio de desenvolvimento da capacidade de processamento de informação bem como da capacidade de análise de questões complexas, usando múltiplas fontes de informação em contexto multidisciplinar.

1.2. METODOLOGIA

De modo a atingir os objetivos específicos pretendidos e responder às perguntas de investigação enunciadas, optámos por uma metodologia de investigação assente em pesquisa exploratória.

Optámos pela revisão da literatura relevante de modo a enquadrar conceitos-chave do tema analisado. Para tal foi efetuada a pesquisa e interpretação de literatura nacional e internacional, a pesquisa bibliográfica incidiu sobretudo de artigos científicos, monografias, dissertações, legislação nacional e europeia sobre a temática.

1.3. ESCOLHA E JUSTIFICAÇÃO DO TEMA

O tema da presente dissertação no âmbito do mestrado em Segurança e Justiça é “Videovigilância: prevenção de incivilidades através de sistemas de videovigilância inteligentes”.

A escolha do presente tema foi elaborada tendo em consideração a pertinência e a atualidade que o mesmo tem na sociedade hodierna: urbana e tecnológica.

1.4. DELIMITAÇÃO DO OBJETO DE ESTUDO: OBJETIVO GERAL

O tema a partir do qual o presente trabalho se desenvolverá é: “Videovigilância: prevenção de incivildades e criminalidade violenta através de sistemas de videovigilância inteligentes”. Desperta a pergunta de partida: “Qual é o estado da arte sobre a utilização de IA nos processos de videovigilância utilizando CCTV para fins de prevenção criminal?”

Com esta investigação pretendemos explorar os possíveis benefícios da introdução de ferramentas e softwares tecnológicos, mais precisamente Inteligência Artificial (IA), nos sistemas de videovigilância de modo a melhorar a prevenção criminal, particularmente para maximizar a prevenção de criminalidade violenta e organizada. Dada a generalização do uso de sistemas de videovigilância tanto em número como em meio de utilização, decidimos concentrar o esforço desta investigação delimitando o objeto de investigação. O espaço público será o foco da investigação.

1.5. DELIMITAÇÃO DO OBJETO DE ESTUDO: OBJETIVO ESPECÍFICO

Para dar resposta à pergunta de partida definiram-se os seguintes objetivos específicos:

Verificar a correlação entre a implementação de sistemas de videovigilância e a prevenção à prática criminal;

Analisar o impacto da videovigilância no sentimento de insegurança;

Analisar os benefícios da inteligência artificial na videovigilância para a prevenção de incivildades e criminalidade violenta.

1.6. PERGUNTAS DE INVESTIGAÇÃO

Para melhor delinear a linha de pensamento da presente investigação e maximizar a clareza dos argumentos, definimos um conjunto de perguntas de investigação derivadas diretamente dos objetivos específicos acima explanados.

Qual o contributo da videovigilância na prevenção de criminalidade?

Qual o impacto da videovigilância no sentimento de insegurança da população?

De que modo poderia a Inteligência artificial aplicada à videovigilância aumentar a eficiência da resposta policial?

1.7. ESTRUTURA DA DISSERTAÇÃO

O conteúdo e desenvolvimento da presente dissertação será subdividido em oito capítulos.

O primeiro capítulo expressa o enquadramento teórico da presente dissertação; enquadra o desenvolvimento expositivo a uma área temática específica, procede à delimitação geral e específica do tema em estudo, à especificação das perguntas de investigação e da metodologia utilizada para as responder.

O segundo capítulo versa sobre as questões sociais incluídas na problemática da prevenção da criminalidade e incivildades. Começando por discorrer sobre a componente ética e moral do ser humano, apresenta conceitos basilares para o funcionamento em comunidade: a normal moral e a norma jurídica. Em seguida apresenta perspetivas filosóficas acerca da natureza humana. A partir destes elementos funcionais, passa para a apresentação do desvio, do crime e das incivildades como formas que atentam contra a segurança pública. Para minimizar a ocorrência e impacto destes fenómenos avançamos para a apresentação de perspetivas para a sua prevenção.

O terceiro capítulo versa sobre as questões tecnológicas que podem ser utilizadas para a prevenção de eventos que lesam a segurança pública. Para a prevenção da criminalidade e das incivildades, expomos o potencial do efeito panóptico gerado pela videovigilância no comportamento dos agentes e apresentamos a Inteligência Artificial como meio coadjuvante. Seguidamente apresenta o conceito de *Smart city*, como a cidade que se pretende adepta da internet das coisas e por isso inteligente.

O quarto capítulo versa sobre as questões relacionadas com a interseção entre as Políticas de Segurança e a Administração Pública. Tratando a presente dissertação questões de segurança pública é importante apresentar conceitos essenciais relacionados com o tema, nomeadamente introduzindo o conceito de Administração Pública, o conceito de Política Pública e o conceito de Políticas de Segurança.

O quinto capítulo introduz os principais temas analisados na presente dissertação: a criminalidade, o CCTV (*Closed Circuit Television*) e a IA. Também apresentamos as conclusões elaboradas pelo Relatório Anual de Segurança Interna de 2023.

O sexto capítulo apresenta as vulnerabilidades humanas e tecnológicas associadas aos sistemas de CCTV, apresenta também o enquadramento jurídico português aplicável ao CCTV, bem como o enquadramento jurídico geral português e da comunidade relativo ao uso da Inteligência Artificial em sistemas CCTV.

O sétimo capítulo faz referência a cidade de Lisboa como possível laboratório experimental, nomeadamente o Bairro Alto.

O oitavo e último tece considerações finais acerca da utilização de CCTV inteligência para a prevenção de incivildades e criminalidade.

2. NATUREZA HUMANA, SOCIEDADE, CRIME

Embora utilizados de forma aparentemente intercambiável, os conceitos de Moral e Ética são distintos. Interligados, mas distintos entre si, Moral e Ética correspondem a diferentes dimensões da codificação da ação Humana.

Ēthos em grego possui duas grafias: *ἦθος* (*ēthos*) e *ἔθος* (*ethos*), essa dupla grafia não é despiciente. Segundo Figueiredo e Guilhem (2008) a dupla grafia encerra em si três significados distintos: abrigo, índole e costumes.

O termo *ἦθος* (*ēthos*) tem dois significados, dependendo do contexto em que é empregue, pode ter o significado de abrigo ou morada como ter o significado de índole ou caráter. Quanto ao primeiro significado- abrigo ou morada- este deriva do uso do vocábulo, primeiramente em contexto literário, para expressar locais de abrigo. Relativamente ao segundo significado- índole ou caráter- este é utilizado para expressar a natureza do homem na vida, o seu caráter; esta dimensão debateu Aristóteles em “Ética a Nicómaco”.

Em contrapartida o termo *ἔθος* (*ethos*) reporta a dimensão social do ser, alude aos costumes e hábitos concretos do Homem como ser social.

“Antes de Aristóteles, estas palavras [*ēthikos* e *ēthos*] não tinham qualquer significado filosófico ou teológico e referiam-se apenas ao costume ou contextos habituais (hábitos e habitats).” (Heimbach, 2015, p.2) Segundo Heimbach (2015) a palavra Ética surgiu a partir do adjetivo *ēthikos*, este por sua vez sendo a adjetivação da palavra *ēthos*, desde a alusão destes vocábulos na obra aristotélica “Ética a Nicómaco”, o significado destes termos evoluiu e extravasou o significado original enunciado por Aristóteles.

A Ética releva a estruturação teórica do dever ser, a esta importa indagar sobre a definição daquilo que deve ser considerada a conduta humana certa e aquilo que define a existência virtuosa.

A subtileza do termo *Ēthos* e as suas diversas aceções foram perdidas quando foram adaptadas ao latim. *Moralis* assumiu tanto a vertente da índole como do costume do vocábulo *Ēthos*.

O termo Moral releva para os códigos, condutas e costumes específicos de determinados indivíduos ou grupos.

Como disse já Camões: “Mudam-se os tempos, mudam-se as vontades, (/) muda-se o ser, muda-se a confiança; (/) todo o mundo é composto de mudança, (/) tomando sempre novas qualidades.” (Camões, 1971, p.79). Como tal, as normas morais e normas jurídicas prescrevem os preceitos e princípios que norteiam a conduta humana em sociedade, a sua natureza é eminentemente volúvel. Pois a única constante da vida é a mudança, todo o organismo, seja ele animado ou inanimado, está em constante evolução. Essa mudança pode ser mais visível ou menos visível, pode ser mais veloz ou menos veloz, mas nada é eterno.

A norma moral prescreve comportamentos. A norma moral é gerada espontaneamente por um grupo específico de indivíduos por forma a gerir a conduta interpessoal dentro da comunidade em particular, define aquilo que deve ser considerado moral ou imoral e é mantida e transmitida sobretudo através da oralidade.

Por seu turno, a norma jurídica prescreve condutas permitidas, condutas proibidas e uma sanção associada à prática de condutas proibidas. A norma jurídica, baseada na vontade geral da comunidade, é produzida por um corpo superior que as impõe através de meios coercivos. Ambas derivam fundamentalmente a sua essência da ética, mas a sua natureza é distinta.

Em relação à natureza humana, a perceção pode ser díspar: egoísta e hedonista ou simples e pacífica. Thomas Hobbes (2005, p.46) argumenta que embora haja pequenas variações individuais entre os indivíduos, os homens são tão iguais em termos de qualidades físicas e mentais que não podem reclamar a si benefícios exclusivos; a vaidade e o egocentrismo tornam essa igualdade inaceitável. Dessa igualdade, defende o autor, surge uma inimizade que impede o convívio pacífico entre os homens,

Porque cada um pretende que seu companheiro lhe atribua o mesmo valor que ele se atribui a si próprio e, na presença de todos os sinais de desprezo ou de subestimação, naturalmente se esforça (...) por arrancar de seus contendores a atribuição de maior valor, causando-lhes dano. (Hobbes, 2005, p.48)

Jean-Jacques Rousseau (1761) concebe a natureza humana a partir do homem pré político. Esse homem deambulava pelas florestas, desconhecia a linguagem, desconhecia a indústria, era um ser simples nos modos e pacífico no trato com os demais.

Os homens nesse estado [selvagem], não tendo entre si nenhuma espécie de relação moral nem de deveres conhecidos, não podiam ser bons nem maus, nem tinham vícios nem virtudes, a menos que, tomando essas palavras em um sentido físico. (Rousseau, 1761, p.66)

A inteligência e a capacidade de escolha diferenciam o Homem do restante mundo animal. A liberdade natural oferece ao Homem a possibilidade de tudo fazer e tudo dispor, em estado natural, a ação humana tem como única condicionante a Natureza. Contudo, no contexto do livre exercício dos seus apetites o Homem tem de coagir os seus semelhantes, ou no reverso se não dispuser de meios para impor a sua vontade, sofrer coerção por parte dos seus semelhantes. Para livrar-se da violência exercida pelos seus semelhantes e proteger os seus haveres, o Homem foi forçado a associar-se. A Comunidade política é um elemento necessário ao desenvolvimento da inteligência e a capacidade de escolha, esta é:

O meio de que a natureza se serve para levar a cabo o desenvolvimento de todas as disposições [do homem] é o seu antagonismo na sociedade [...]. Entendo aqui por antagonismo a sociabilidade insociável dos homens, isto é, a sua tendência para entrarem em sociedade, tendência que, no entanto, está unida a uma resistência universal que ameaça dissolver constantemente a sociedade. (Kant, 1992, p.25)

Ao formar uma sociedade ele perde a sua liberdade natural, mas ganha a liberdade civil.

2.1. DESVIO E CRIME

Nem tudo aquilo que difere é necessariamente mau; os membros de uma determinada sociedade têm um conjunto específico de normas que ditam o comportamento dos seus constituintes, da parte destes é esperado o cumprimento dessas normas. Quando o indivíduo não corresponde com aquilo que lhe é expectável e age diferentemente daquilo que está convencionado, incorre num desvio da norma.

Maurice Cusson (2011) descreve que a desviância é o termo usado na sociologia para designar as condutas e estados que violam normas sociais; essas normas têm importância suficiente para que os membros do grupo sancionem os incumpridores.

As normas ditam aquilo que é expectável e normal. Aquilo que é definido como normal varia no tempo e no espaço, por esse motivo em abstrato podemos considerar que a “normalidade envolve um conjunto partilhado de valores e normas culturais ou normas acerca da forma de comportamento, indumentária ou pensamento.” (Henry et Howard, 2019, p.13)

Quando um determinado tipo de ação não está em conformidade com o expectável, podemos falar de desvio. Ora o desvio pode tanto ser positivo como negativo, pois toda a ação pode produzir efeitos positivos e negativos. O foco da presente investigação será o desvio negativo. Desvio corresponde ao incumprimento das normas fixadas por uma determinada sociedade, o crime corresponde a uma forma particular de desvio.

Aquilo em que consiste o crime resulta da construção social e sociológica dos comportamentos considerados reprováveis o suficiente para que os mesmos sejam alvo de codificação e sanção. Porque toda a ação acarreta virtuais benefícios e virtuais prejuízos, quando a prática de determinados comportamentos é considerada prejudicial para a manutenção da ordem pública e para a conservação do tecido social, a coletividade determina que tais comportamentos não são toleráveis e devem ser reprovados.

Genericamente de uma perspectiva legalista, constitui crime toda a prática deliberada de um ato explicitamente declarado, proibido, ilícito e punido pelo direito penal, que é considerado nocivo e prejudicial para a sociedade. De acordo com esta perspectiva, para que um ato seja considerado crime deverá existir um enquadramento jurídico, ou seja, a prática criminosa deve estar tipificada. Nesta senda, “crime é um ato intencional que viola a lei penal (legislação e jurisprudência), cometido sem defesa ou desculpa e penalizado pelo Estado como crime ou contraordenação.” (Tappan, 1947, p. 17)

Dada a irrefreável evolução da sociedade, as normas sociais que dão origem às normas jurídicas estão em constante evolução; aquilo que é criminalizado varia consoante o local e o período histórico. Face à relatividade da lei, outros autores concebem o crime numa ótica diferente. Recusando a via restritiva da visão legalista, outros autores desenvolveram perspectivas assentes numa lógica sociológica.

Genericamente de uma perspectiva sociológica constitui crime toda a prática de um ato que ofende a moralidade coletiva e produz uma intensa indignação nos membros da coletividade. Émile Durkheim (1991, p.89) caracteriza crime como um ato que apesar de ofender o sentimento coletivo, é normal e útil para a evolução normal da moral e do direito. A ênfase é colocada nas relações sociais e nas normas criadas para regular as relações sociais, por isso crime “é fundamentalmente uma violação de normas de conduta que contêm sanções, quer se encontrem [tipificadas] no direito penal de um Estado ou apenas como regras de funcionamento de grupos sociais.” (Reckless, 1940, p.10)

Esta perspectiva acomoda a variação temporal e espacial daquilo que constitui crime, contudo pretere a análise das relações de poder dentro da comunidade.

2.2. INCIVILIDADES

A ética expressa o dever ser, produz imperativos que ditam a ação do agente. Estes imperativos podem ser hipotéticos, os quais ordenam determinada ação como meio para chegar a um determinado fim, ou podem ser categóricos, estes prescrevendo o cumprimento de determinada ação, independentemente da vontade do agente e de virtuais benefícios que poderiam derivar.

Diferentemente, o Direito expõe normas formais com mecanismos sancionatórios que prescrevem a conduta humana em sociedade política, o “direito objetivo é o conjunto de regras de comportamento social cujo cumprimento é imposto, pela autoridade, com aplicação de sanções àqueles que deixarem de as cumprir.” (Martins, 1970, p.9)

Na encruzilhada entre o dever ser que a ética impõe e dever agir que o Direito obriga estão as incivildades; nem crime ou contraordenação, mas nem tão pouco aceitável em sociedade.

Goffman (1963) considera que o comportamento público dos indivíduos é guiado por um conjunto de normas que o mesmo designa como propriedades situacionais (*situational proprieties* termo original), as normas existem para regular o comportamento em público, estas variam de acordo com a familiaridade entre os sujeitos e a situação em causa. Os

indivíduos seguem as normas e agem de determinada forma para exprimir a sua relação com uma comunidade.

“[As] propriedades situacionais têm um caráter moral: o indivíduo é obrigado a conservá-las(...) e se este falhar, desenrola-se algum tipo de reconhecimento público do seu fracasso. (Goffman, 1963, p.240) Essas faltas demonstram aquilo que o autor refere como “falta de respeito” ou “falta de orgulho” que denotam a alienação do sujeito da comunidade. (Goffman, 1963) Daqui emerge a noção de comportamento inserido nos limites da urbanidade.

Atendendo ao facto de as incivildades representarem não só violações dos códigos de conduta sociais como o uso abusivo e destrutivo do espaço, Hunter refere que estes atos “podem pôr em causa a própria ideia básica de que, enquanto cidadão, se vive sob a proteção e segurança de uma “sociedade civil” ordenada.” (Hunter, 1978, p.5)

Desenvolvendo esta linha de pensamento, Wilson e Kelling (1982) depois de terem analisado os resultados da implementação de um programa de policiamento de proximidade- "Safe and Clean Neighborhoods Program", - concluíram que apesar de a criminalidade reportada não ter diminuído, ocorreu um aumento do sentimento de segurança graças ao policiamento de proximidade. Segundo os autores (Wilson e Kelling, 1982) apesar de o principal receio dos cidadãos compreender ser atacado aleatoriamente por estranhos, existe outro fator a ter em conta: o medo de ser perturbado por pessoas desordeiras.

Ao nível da comunidade, a desordem e a criminalidade estão normalmente indissociavelmente ligadas, numa espécie de sequência de desenvolvimento. Se a janela de um edifício tiver sido partida e não for reparada, em breve todas as outras janelas serão partidas. (Wilson e Kelling, 1982, p.33)

A prática de incivilidade está diretamente relacionada com a quebra dos sistemas de controlo informais. No contexto norte-americano, em oposição ao contexto europeu, a tónica está na prevenção da ocorrência de tais fenómenos através do policiamento de proximidade e nessa tarefa

A essência do papel da polícia na manutenção da ordem é reforçar os mecanismos de controlo informal da própria comunidade [pois] a polícia não

pode, sem afetar recursos extraordinários, substituir esse controlo informal.”
(Wilson e Kelling, 1982, p.5)

A adaptação do conceito à realidade europeia manteve a essência infra penal, contudo perdeu a natureza pragmática e comunitária, por outras palavras “a europeização do conceito [de incivildades] consistiu em conferir-lhe um alcance teórico sociológico.” (Millburn, 2000, p.337) No processo de europeização do conceito de incivildade verificou-se não só a abstração do pragmatismo local norte-americano como a nacionalização de normas e costumes sociais locais; a incivildade passou a referir-se “as regras de civismo que se presume serem homogêneas numa nação.” (Millburn, 2000, p.337)

Para caracterizar o conceito de incivildade, Roché (2002) subdivide a ação humana em três tipos diferentes de acordo com o objetivo que a despoleta: a ação pode ser aquisitiva, conflitante ou demonstrativa. A ação aquisitiva tem por objetivo adquirir uma vantagem económica, a ação conflitante tem por objetivo manifestar superioridade sobre outrem e a ação demonstrativa tem por objetivo exibir o agente.

Roché (2002) exclui toda a manifestação de agressão física do campo da incivildade, considera também que, de forma geral, as ações aquisitivas nem os comportamentos privados se enquadram no âmbito da incivildade; a incivildade é eminentemente uma ação demonstrativa que pode ser ilegal ou legal.

A diferente caracterização deste fenómeno deve-se segundo Millburn (2000) ao desigual posicionamento tomado tendo em consideração o princípio da legalidade e também do tratamento judicial que deve ser conferido às manifestações deste fenómeno. Segundo o autor, (Millburn, 2000), por uma parte esta noção apresenta a vantagem de permitir apreender atos que não estão abrangidos pelo código penal, mas que constituem uma forma de perturbação da ordem social e devem ser adereçados e por outra parte indica que pode ser útil conceptualizar um conjunto de atos peri-judiciais mas o seu tratamento não deve ser contemplado no âmbito da ação pública.

Cusson define “incivildades [como] um conjunto heterogêneo de ‘peri-delitos’ e de sinais de deterioração que assinalam aos transeuntes a presença de perigo difuso nas ruas, nos parques e noutros lugares públicos.” (Cusson, 2011, p.191)

Os conceitos avançados por diversos autores divergem, contudo entre as diversas concepções de incivildade podemos apreender duas dimensões omnipresentes: estas são geradas a partir da rutura dos laços sociais de uma comunidade, contribuindo para a contínua erosão dos laços sociais, estas representam comportamentos que demonstram falta de urbanidade e ainda que os comportamentos através dos quais se materializam são dificilmente juridicamente sancionados.

“A ideia geral é que as incivildades podem minar a vida social e constituir a base para o desenvolvimento da violência e da delinquência.” (Damon, 2000, p.140)

2.3. SEGURANÇA PÚBLICA

No estado solitário e natural, o maior inimigo do bem-estar humano são os elementos. Contrariamente, em estado social e artificial, as condicionantes físicas do meio deixam de representar a maior ameaça à tranquilidade do ser humano; o maior inimigo torna-se o congénere com o qual o Homem partilha o espaço. Porque “o primeiro sentimento do Homem foi o da existência, o seu primeiro cuidado, o da conservação” (Rousseau, 1761, p.33), importa, portanto, afirmar a segurança como uma necessidade coletiva.

Segurança deriva do termo latino *securitate*, originalmente caracterizava um estado de liberdade de preocupação e ansiedade. Clemente define a segurança” como o estado de tranquilidade resultante da ausência de perigo ou, pelo menos, da percepção real de risco.” (Clemente, 2010, p.155)

Simbióticas em termos de interação e aparentemente contraditórias em natureza estão a segurança e a liberdade; uma não existe sem a outra e nenhuma pode sobrepor-se sob perigo de destruir a essência da homóloga.

A liberdade natural, ou como Bauman (1989) designa por “liberdade completa” representa uma concepção hipotética, uma experiência mental que só pode ser exercida em “plena solidão: abstenção total de comunicação com outras pessoas.” (Bauman, 1989, p.84) A ficção que é a pura liberdade é contraproducente, os hipotéticos ganhos obtidos da máxima liberdade de ação seriam anulados, por um lado, pela maximização das forças da natureza

sobre o físico humano e pela restrição à ação que a livre e solitária prossecução de objetivos acarreta. Por outro lado, a natureza social do ser humano não teria quadro para a sua plena realização.

Para possibilitar a plena realização do potencial cognitivo e social do ser humano é necessário proteger os membros de uma sociedade dos comportamentos antissociais levados a cabo entre associados, para cumprir essa função no aparelho regulador- Estado- é delegada a tarefa de garantir a tranquilidade pública.

A Constituição da República Portuguesa, ora em diante designada por CRP, é a primeira fonte de Direito a nível nacional. A CRP constitui a garantia dos direitos e liberdades fundamentais como uma das tarefas fundamentais do Estado e na sua parte I reconhece e elenca um vasto conjunto de direitos fundamentais. Entre esses direitos fundamentais estão o direito de liberdade, de segurança, de participação política e os direitos de natureza económica, social e cultural.

A CRP no disposto do art.º 27º refere-se ao direito à liberdade e à segurança, enunciando que

Todos têm direito à liberdade e à segurança [e que] ninguém pode ser total ou parcialmente privado da liberdade, a não ser em consequência de sentença judicial condenatória pela prática de ato punido por lei com pena de prisão ou de aplicação judicial de medida de segurança. (Constituição da República Portuguesa, 1976)

Como podemos observar a partir da formulação semântica da Constituição, a liberdade e a segurança são elencadas em simultâneo, o seu exercício não é irrestrito, mas sim exercido em complementaridade: “o direito à segurança forma um todo com o direito à liberdade – não há segurança dissociada da liberdade.” (Clemente, 2010, p.144)

O Estado, como unidade política, utiliza o seu poder político para satisfazer os interesses gerais que a coletividade considera primordiais, mormente a segurança das pessoas, bens materiais e dos valores, a justiça no relacionamento entre os membros do grupo e o bem-estar material e espiritual.

A segurança é erroneamente associada à coação jurídica e material, à restrição de direitos, liberdades e garantias. A segurança não deve ser encarada exclusivamente através de uma

perspetiva repressiva, que realça a sua dimensão coerciva, mas também através de uma perspetiva humanista: a segurança como bem jurídico coletivo garantístico do exercício dos direitos, liberdades e garantias.

A segurança presentemente enunciada corresponde à segurança na sua dimensão interna e pública, a dimensão da defesa e manutenção das normas jurídicas- emanadas da ordem social dominante- de um corpo social e jurídico.

Impende sobre o Estado criar as condições para a manutenção da segurança interna, tal significa assegurar

A ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática. (Lei n.º 53/2008, 2008)

A CRP é textualmente omissa relativamente à noção de ordem pública, contudo para a manutenção do regular funcionamento do Estado e para a concretização dos fins aos quais se propõem está implícito que “a ordem pública apresenta-se como um princípio pré-constitucional e supraconstitucional, inerente ao próprio Estado.” (Sousa, 2023, p.135) Princípio pré-constitucional e abrangente, nas palavras de Sousa (2023) a ordem pública engloba em termos mais ou menos restritivos a segurança pública, a tranquilidade pública e a salubridade pública; a segurança implica a proteção do cidadão contra os perigos naturais e resultantes da conduta humana, a tranquilidade garante ao cidadão uma vida pacífica e a salubridade implica assegurar uma vivência sadia.

Os termos ordem pública e segurança pública são verossimilhantes, mas distintos.

A ordem pública “compreende as normas não escritas de conduta relativas a valores sociais relevantes e partilhados pela maioria da coletividade” (Sousa, 2023, p.372), a sua natureza não é artificial e tem “uma origem biológica, anterior à emergência da comunidade política.” (Clemente, 2010, p.155)

A doutrina jurídica portuguesa, materializada pela Procuradoria-Geral da República (1996) citada por Clemente (2010) define a ordem pública como o “conjunto das condições externas necessárias ao regular funcionamento das instituições e ao pleno exercício dos direitos

individuais, nuclearmente segundo a trilogia funcional da defesa da tranquilidade, segurança e salubridade.” (Parecer nº 9/96-B/ Complemento de 12-01-2000, 2000. p.1970)

Diferentemente, a segurança pública compreende “as normas escritas [que são] parte integrante do ordenamento jurídico objetivo” (Sousa, 2023, p.372), são normas jurídicas positivadas cuja função é defender o Estado e as suas instituições e garantir o respeito pelas normas jurídicas.

Para garantir a inviolabilidade das normas jurídicas e manter a ordem pública, cabe ao Estado fazer cumprir; a contenção da conduta humana dentro de parâmetros legais e aceitáveis de modo a preservar a segurança pública. Para atingir esse fim, é necessário criar medidas de modo a fornecer orientação ao sujeito e garantir a vigilância do transgressor. Bauman concebe duas vias para atingir esse fim, exemplificando que “podemos colocar as pessoas numa situação que as impeça de fazer coisas que não queremos que façam; ou colocá-las numa situação que as encoraje a fazer coisas que queremos que façam.” (Bauman, 1989, p.23)

Os indivíduos podem ser conduzidos a agir de acordo com as normas através de duas formas: incentivo ou prevenção. Segundo Bauman (1989) o incentivo reporta ao procedimento que depreende que o agente, munido de autonomia, possuindo autocontrole, usa a sua liberdade para agir de acordo com a ordem das coisas. Por outro lado, segundo Bauman (1989) a repressão reporta ao sistema que crê que o agente necessita uma força de controlo externa e arregimentação, caso contrário tende para agir violando preceitos dispostos pela ordem das coisas.

Para prevenir fenómenos antissociais, mais precisamente comportamentos que atentam contra a segurança pública, bem como para reduzir os custos da criminalidade- económicos, sociais e com o sistema de justiça penal-, é fundamental apostar no desenvolvimento de políticas, táticas e estratégias tendentes à prevenção da criminalidade.

Sousa estabelece duas tipologias de medidas criadas pela Administração para combater ilícitos: as medidas podem ter como finalidade reprimir o ilícito e, por conseguinte, têm natureza repressiva ou podem ter como finalidade prevenir o ilícito, e nesse caso ser consideradas preventivas (Sousa, 2023). Similarmente Cusson considera que se enquadram na prevenção criminal “as intervenções não penais sobre as causas próximas dos delitos que

têm o objetivo específico de reduzir o seu risco ou gravidade” (Cusson, 2011, p.197) A repressão é diferente “tem um forte caráter penal, reativo e público.” (Cusson, 2011, p.197)

Por sistema judicial entende-se, habitualmente, o conjunto de autoridades e organismos responsáveis pela proteção dos direitos das pessoas à segurança e ao gozo dos direitos consagrados juridicamente. Em Portugal integram o sistema de justiça criminal

O Ministério Público, os Juízes, os advogados, os órgãos de policial criminal, os serviços de execução das sanções criminais, serviços de apoio às vítimas, Instituto Nacional de Medicina Legal e Ciências Forenses e o Laboratório de Polícia Científica da PJ [Polícia Judiciária]. (Ministério da Justiça, 2024).

Ao Ministério Público, conforme expresso no artigo 219º da CRP,

Compete representar o Estado e defender os interesses que a lei determinar, bem como participar na execução da política criminal definida pelos órgãos de soberania, exercer a ação penal orientada pelo princípio da legalidade e defender a legalidade democrática. (Constituição da República Portuguesa, 1976)

A este órgão, titular da ação penal, compete defender a sociedade e os direitos juridicamente consagrados. A este órgão compete especificamente

A receção de denúncias, queixas e participações e apreciação do respetivo seguimento; a direção do inquérito; a prolação de despacho; a sustentação da acusação na instrução e no julgamento; a promoção da execução das penas e das medidas de segurança (Ministério Público, 2024)

e com interesse na defesa também pode interpor recursos.

Os tribunais, órgão que incorpora os Juízes, conforme expresso no artigo 202 da CRP “são os órgãos de soberania com competência para administrar a justiça em nome do povo”(Constituição da República Portuguesa,1976) e a estes compete “assegurar a defesa dos direitos e interesses legalmente protegidos dos cidadãos, reprimir a violação da legalidade democrática e dirimir os conflitos de interesses públicos e privados.” (Ministério da Justiça, 2024).

O sistema judicial tem natureza e *modo operandis* diferente da prevenção criminal; um pune o outro precave. Schneider (2015) evidencia essas diferenças, considerando que o sistema judicial, através das organizações estatais, intervém e reage sobretudo sobre o ofensor depois da consumação do crime; contrariamente, a prevenção criminal tem como foco a intervenção em potenciais ofensores e vítimas, procurando através de mecanismos formais e informais, organizações estatais e privadas proactivamente impedir a ocorrência de ilícitos.

Sem descurar a importância que o sistema de justiça penal desempenha para a manutenção do Estado de Direito e da segurança jurídica, a sua intervenção na sociedade recai sobretudo no âmbito repressivo.

2.3.1. PREVENÇÃO CRIMINAL

A prevenção criminal procura reduzir a ocorrência de crime através da redução das oportunidades para que tal ocorra ou através do tratamento dos fatores que propiciam o comportamento criminal. O público-alvo são as comunidades, as famílias e os indivíduos que, a partir da análise de dados concretos, apresentem elevados fatores de risco criminal.

Petrosino et al., 2010; Bales e Piquero, 2012 citados por Stephen Schneider (2015, p.10) reportam que as sanções da justiça penal e o encarceramento, em particular, não têm um impacto significativo na prevenção da reincidência.

No tocante à interseção entre a prevenção criminal e o sistema de justiça criminal, considerando a grande diversidade de definições de prevenção de criminalidade, é possível subdividi-las em duas grandes abordagens: as concepções abrangentes e as concepções limitadas. As concepções abrangentes defendem que todo o ciclo de vida do crime pode ser incorporado na prevenção, já concepções limitadas defendem que a prevenção incorpora as ações que ocorrem anteriormente à prática de um crime.

Pease (1997) distingue três perspetivas explicativas das causas do crime: perspetivas que assumem que o crime resulta da estrutura física e social, perspetivas que consideram que o crime resulta do funcionamento da psique humana e perspetivas que consideram que as circunstâncias são precursoras do crime.

De entre as teorias que se enquadram na categoria que considera que o crime resulta da estrutura física e social, já evidenciamos a Teoria das Janelas Partidas de Wilson e Kelling. Outras teorias que contribuirão para o debate também serão explanadas.

A Teoria das Atividades de Rotina, desenvolvida por Lawrence Cohen e Marcus Felson evidencia a importância do tempo, do ritmo e do *timing* para a ocorrência da prática criminal. Considerando que estes aspetos haviam sido anteriormente negligenciados no estudo da criminologia, os autores defendem que para a prática de atividades ilegais é necessária a justaposição espacial e temporal de três fatores: “(1) infratores motivados, (2) alvos adequados, e (3) a ausência de guardiões capazes de combater uma violação.” (Cohen e Felson, 1979, p.589)

Um modelo diferente no tocante à prevenção criminal é a teoria defendida por Herman Goldstein. O autor considerou que a Polícia como organização, a par outros organismos públicos “correm o risco de ficar tão preocupadas com a gestão das suas organizações e tão envolvidas nos seus métodos de funcionamento que perdem de vista os objetivos para os quais foram criados.”(Goldstein, 1979, p. 237) A função da Polícia é resolver problemas, e “por problemas, refiro-me a uma gama incrivelmente vasta de situações problemáticas que levam os cidadãos a recorrer à polícia.”(Goldstein, 1979, p. 242) Para resolver esses problemas o Policiamento Orientado para os Problemas (POP), propõem um conjunto de soluções.

Considerando que o crime é cometido por agentes conscientes e motivados e que os mesmos cometem o crime em locais específicos surge uma diferente perspectiva relativamente à prevenção criminal. A Teoria dos Padrões Criminais considera que (Brantingham e Brantingham, 1981) o padrão de criminalidade segue a dimensão geográfica dos padrões de atividade humana; a geometria do crime inclui o espaço de atividade, mormente o local familiar onde o criminoso se sente confortável para cometer ofensas.

Tendo por foco outro aspeto, Clarke e Cornish desenvolveram a Teoria da Escolha Racional. Focando-se no processo de escolha racional e intencional dos ofensores, Clarke e Cornish (1985) consideram que a prática criminal implica, por mais rudimentar que seja a racionalidade do agente, a tomada de decisões e escolhas, tendo em conta diversas condicionantes e que é mediante as pistas ambientais do contexto que os ofensores decidem cometer ou não o crime.

Tendo como foco a prevenção da criminalidade através da manipulação do ambiente físico, vários autores, citados por Saraiva et al (2019), como Mayhew et al (1976), Gardiner (1978), Brantingham and Brantingham (1981), Moffat (1983), Crowe (1991), Clarke (1997) ou Cozens et al (2005) debateram e trabalharam estes conceitos adaptando-os às várias fases de evolução da disciplina. A Prevenção Criminal através do Espaço Construído (do inglês *Crime Prevention Through Environmental Design – CPTED*) defende que “um espaço seria mais seguro se tivesse i) uma clara distinção entre a vertente pública e privada; ii) vigilância natural por parte dos legítimos utilizadores e iii) movimento suficiente.” (Saraiva et al, 2019, p.73)

Quanto à conceção daquilo que constitui a prevenção criminal, a prevenção criminal é definida por Ekblom como "uma intervenção nos mecanismos que causam eventos criminais, de forma a reduzir a probabilidade de ocorrência de crimes." (Ekblom, 1996, p.4)

Já Tolan et al. consideram que devem ser consideradas prevenção criminal “as ações destinadas a evitar a génese de atividades criminosas em indivíduos ou a ocorrência de atividade criminosa num determinado local.” (Tolan et al., 2002, p.109)

Nesse aspeto é necessário diferenciar as diferentes modalidades de prevenção criminal. Brantingham e Faust (1976) desenvolveram uma classificação tripartida da prevenção criminal, adaptando do modelo epidemiológico, concebem a prevenção criminal em três níveis: primário, secundário e terciário.

A prevenção primária da criminalidade “identifica as condições do ambiente físico e social que proporcionam oportunidades ou precipitam atos criminosos.” (Brantingham & Faust, 1976, p.290) O alvo deste tipo de tática de prevenção criminal é alterar as condições físicas e sociais que propiciam a ocorrência de fatos delituosos. A prevenção secundária da criminalidade “consiste na identificação precoce de potenciais delinquentes e procura intervir [por forma a que] nunca cometam uma infração penal;” (Brantingham & Faust, 1976, p.290) o seu foco é detetar potenciais infratores e agir sobre os mesmos, seja através de incentivo ou outras ferramentas, de modo que a potencialidade infratora contida no agente não se manifeste. O agente propriamente dito, como autor de determinados atos antissociais, é o foco da intervenção. O último nível traçado pelos autores ultrapassa o meio físico envolvente, as condicionantes sociais, os potenciais delinquentes, envolve já o ofensor. A

prevenção terciária da criminalidade implica uma intervenção nas suas vidas [infratores reais] de forma que não cometam mais crimes.” (Brantingham & Faust, 1976, p.290)

Inspirados pela teoria das atividades rotineiras, Van Dijk e De Waard (1991) adicionaram uma nova dimensão- o público-alvo - a cada um dos três níveis de prevenção criminal de prevenção criminal.

3. VIDEOVIGILÂNCIA

Acompanhando a evolução da sociedade, dos fenómenos sociais e criminais e para obter melhores resultados face ao aumento do escrutínio público, à crescente influência da opinião pública e à rápida e crescente mutação das atividades criminais, as Forças de Segurança têm vindo a adaptar os seus métodos e técnicas à revolução tecnológica.

A vigilância policial ou policiamento tem como principal fim a prevenção de perigos que possam ameaçar bens jurídicos suscetíveis de proteção. Face ao aumento da criminalidade em contexto urbano, aliada ao anonimato prevalente à cidade, a videovigilância, aliada à ação do agente da lei, surge como meio preferencial para o combate de fenómenos criminógenos pois esta permite racionalizar os recursos, diminuir o risco para os primeiros intervenientes, graças à informação visual recolhida, aumentar a eficácia da resposta a situações de necessidade e aumentar as hipóteses de detenção em virtude da maior visibilidade dos infratores.

A obra de Jeremy Bentham “*O Panopticon*; ou, A Casa de Fiscalização: contendo a ideia de um novo princípio de construção aplicável a todas as espécies de estabelecimentos, onde todas as pessoas têm de estar sob vigilância e em especial às penitenciárias, às prisões, oficinas industriais, casas de correção, asilos, fábricas, hospícios, instalações para quarentena, hospitais e escolas: com um plano de administração adaptado ao princípio” explora um conceito basilar que se aplica à videovigilância: gerar a impressão no observado que está sendo observado sem que necessariamente seja essa a realidade.

Para criar essa ilusão, Bentham (1995) idealiza a construção de um edifício circular no qual através da segmentação isolada de cada apartamento, conjugada com a arquitetura

centralizada da torre onde estaria localizado o apartamento do inspetor, os internados acreditassem ser permanentemente observados.

Sendo impossível vigiar cada internado a todo o momento, a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária, ele deveria pensar que está nessa condição. Não crendo que se deixado ao seu encargo o indivíduo optaria pelo comportamento desejado e benéfico para a comunidade, de modo a minimizar a hipóteses de o mesmo incorrer em comportamentos indesejáveis ou proibidos deveria ser alcançado o estado no qual “a aparente onipresença do inspetor (...) combinada com a extrema facilidade de sua real presença “(Bentham, 1995, p.12) garantiria o bom comportamento.

No *Panopticon* de Bentham, conforme caracteriza Bauman (1989), a administração intencional das condições através do tratamento científico produz duas classes distintas: os reclusos e os inspetores; entre ambas existe uma oposição entre liberdade/não liberdade e a ação autónoma/ação comandada. Ver sem ser visto; a assimetria do conhecimento entre o inspetor e reclusos significa que o inspetor sabe tudo acerca do recluso enquanto o recluso nada sabe sobre o inspetor.

O *Panopticon* pode ser interpretado como um modelo descritivo da sociedade no seu todo; um modelo em miniatura, confinado a um edifício rotativo. Uma sociedade que, ao contrário da original imperfeita, concentra o zelo controlador nos locais onde ele é necessário, e o exclui dos outros; uma sociedade que elimina o crime, reprime o comportamento socialmente prejudicial, elimina o desperdício industrial; uma sociedade que proporciona a todos os seus membros um ambiente seguro, pacífico e ordeiro. (Bauman, 1989, p.37)

O *Panopticon* é um modelo de vigilância, uma estrutura hipotética passível de ser implementada em instituições variadas, como em casas de correção, prisões, fábricas, hospícios, hospitais ou escolas. Nesses locais a cada indivíduo cabe um espaço individualizado que se quer individualizante de modo a comprometer possíveis fenómenos coletivos, que articulados entre os indivíduos, possam comprometer a superioridade do agente controlador. A eficiência da vigilância é garantida pela economia visual e pela intangibilidade do olhar fiscalizador.

Diferentemente interpreta Foucault o sistema proposto por Bentham; no modelo panóptico de Bentham é extraída uma leitura aplicável à sociedade em geral.

Foucault (Foucault, 2001, p.152) considera que na sociedade disciplinar gerada pelo panóptico, a arte da punição não se atinge nem através do fomento da expiação de transgressões nem através da repressão dos atos interditos, mas a partir da normalização dos comportamentos. O efeito disciplinador do panóptico é obtido essencialmente através de cinco operações distintas (Foucault, 2001): (1) remeter comportamentos e desempenhos individuais a um conjunto padrão que tem como função ser termo indicador, (2) diferenciar os indivíduos em relação à regra geral, (3) proceder à medição e classificação dos indivíduos, (4) constrangê-los ao cumprimento da regra e (5) definir as fronteiras da normalidade.

Antecessores aos sistemas de vigilância remota através de aparelhos eletrônicos, o paralelismo teórico é notório. O *Panopticon*, a sociedade disciplinar e a videovigilância partilham um essencial elemento: o olhar que está sempre presente, unidirecional e inverificável da vigilância por forma a normalizar a conduta daqueles que creem estar sob o ângulo de visão de um observador e dessa forma dissuadir comportamentos desviantes.

O circuito fechado de televisão, ora em diante designado por *Closed Circuit Television* (CCTV), deriva do termo inglês anteriormente mencionado. Na sua génese o termo diferenciava a televisão de sinal aberto e público, por outras palavras a televisão como conhecemos comumente, da televisão de sinal fechado e privado.

Nas palavras de Goold “*closed circuit [of] television* é um sistema no qual um conjunto de câmaras de vídeo estão conectadas num circuito fechado, sendo as imagens produzidas enviadas para um monitor televisivo central ou gravador.” (Goold, 2004, p.12) Fazem parte deste sistema os seguintes elementos (Castillo, 2011) duas ou mais câmaras, monitores, gravadores, sistemas de comutação e rede de transmissão. As câmaras captam a imagem do ambiente físico, os monitores reproduzem a informação captada pelos equipamentos de recolha visual, os gravadores armazenam fisicamente em discos ou imaterialmente em nuvens de informação a informação captada pelas câmaras, o sistema de comutação interliga os diferentes equipamentos de um sistema e a rede de transmissão assegura a transmissão dos sinais de vídeo dentro de uma rede de computadores.

A partir destes elementos basilares, os sistemas CCTV, derivado das diferentes funcionalidades de cada elemento do sistema, apresentam entre si marcadas diferenças. As

câmaras podem ser estáticas, tendo ângulo de captação fixo ou podem ter funcionalidades que permitam a alteração do ângulo de captação. Pode um operador controlar remotamente a câmara ou pode o sistema informático dependendo da programação, se simplesmente com base horária ou com base na deteção automática de movimentação, girar, inclinar ou efetuar zoom e mudar a área captada. Os aparelhos de captação de imagem (e som) podem ser instalados em locais fixos ou podem ser instalados em equipamentos móveis. As características técnicas desses aparelhos têm a maior importância para a qualidade das imagens captadas. O gravador garante o armazenamento da informação captada pelas câmaras. Também importantes no sistema são o sistema de comutação e a rede de transmissão pois garantem a transmissão da informação captada e gravada sem perder a qualidade e sem a intromissão de terceiros.

As imagens captadas pelos sistemas CCTV não têm a função, num Estado de Direito Democrático, de controlar todos os aspetos da vida do cidadão. George Orwell na sua obra “1984” descreveu uma sociedade totalitária fortemente controlada pelo Partido e pela Polícia do pensamento, a visão distópica retratada nesse romance nada tem que ver com a videovigilância existente no Estado de Direito Democrático pois ela é exercida com o fim de preservar os direitos, liberdades e garantias dos cidadãos.

Os sistemas CCTV servem para a proteção e não para a vigilância, por isso apelidamos esses sistemas de videoproteção pois o seu objetivo é proteger o cidadão.

Segundo a Câmara Municipal da Amadora “as câmaras de videoproteção constituem uma ferramenta de grande importância na prevenção e na manutenção da segurança pública na cidade, complementando de forma relevante o trabalho de proximidade desenvolvido” (Câmara Municipal da Amadora, 2022) pelas Forças e Serviços de Segurança.

O sistema facilita a proteção do cidadão através da monitorização de diversos locais em direto da via pública, permitindo a deteção e intervenção precoce em situações de perturbação da segurança pública.

3.1. INTELIGÊNCIA ARTIFICIAL

A Inteligência artificial, doravante mencionada por IA, está atualmente por toda a parte.

A IA apresenta-se como uma funcionalidade tecnológica que permite aumentar a produtividade de determinadas tarefas e melhorar a eficiência humana. Esses benefícios podem ser alcançados através de softwares cuja capacidade de análise e previsão permitem processar grandes quantidades de dados e executar tarefas complexas.

Segundo Haenlein e Kaplan (2019) os primórdios da IA podem ser rastreados a 1939, momento em que Alan Turing criou uma máquina com 213cm por 183cm e 60cm, que pesava 1 tonelada. Essa máquina, considerada como “o primeiro computador eletromecânico funcional” (Haenlein e Kaplan, 2019, p. 6) alcançou aquilo que durante a II Guerra Mundial nenhum matemático conseguira: decodificar o código Enigma, sistema de encriptação utilizado pelas Forças Armadas da Alemanha Nazi.

O artigo científico publicado em 1950 "Computational Machinery and Intelligence" por Alan Turing, pode ser considerado um “artigo de referência” (Haenlein e Kaplan, 2019, p. 7) no domínio da inteligência artificial. Reconhecendo a natureza ambígua da pergunta: As máquinas conseguem pensar? Turing (1950) substituiu o conceito de pensamento pela capacidade de previsão do comportamento humano num “jogo de imitação”; o foco da questão transita para a medição da capacidade de uma máquina imitar bem o comportamento humano. Neste jogo (Turing, 1950) para que a máquina possa ser considerada inteligente e passar o teste, um interrogador humano deve comunicar através de mensagens escritas com um humano e com uma máquina e a partir das respostas produzidas este não deve ser capaz de fazer a distinção de forma fiável entre o humano e a máquina.

Os conceitos são diversos, de uma forma mais sintética, IA pode ser considerada como “o ramo da ciência informática dedicado à criação de sistemas dedicado a executar tarefas que normalmente requerem a inteligência humana.” (Chartrand et al. 2017, p.2114) Mais elaboradamente, Nadikattu considera que a “Inteligência Artificial baseia-se no princípio de que as máquinas podem ser construídas com a capacidade de efetuar tarefas complexas que normalmente requerem conhecimento humano” (Nadikattu, 2019, p. 89) e que tais máquinas “podem aprender com as tendências e experiências do comportamento humano, recolher

dados, analisar e executar processos de uma forma ainda melhor e ter uma precisão superior à dos humanos.” (Nadikattu, 2019, p. 89) Focando na componente prática daquilo que consiste a inteligência em máquinas, a computação inteligente pode ser caracterizada como a capacidade de resolver problemas através da “inferência baseada no conhecimento, o raciocínio com informação incompleta, várias formas de percepção e aprendizagem, e aplicável a problemas como o controle, a previsão, a classificação e a otimização.” (Munakata, 2007, p. 2)

Salientando que o conceito de computação inteligente menciona os termos “conhecimento” e “racionar” aplicados à computação, contudo essas características inerentemente humanas não são passíveis de transposição a aparelhos eletrônicos. Podemos, contudo, entender “conhecimento” como dados e “raciocinar” como a execução de algoritmos, mais precisamente, dado como “elemento inicial de qualquer acto de conhecimento antes de ser elaborado no processo cognitivo” (Priberam, 2024) e algoritmo como “conjunto de regras e operações bem definidas e não ambíguas, que, aplicadas a um conjunto de dados e num número finito de etapas, conduzem à solução de um problema.” (Priberam, 2024)

Também humanizando a capacidade de processamento de dados e inferência de equipamentos eletrônicos, Shubhendu e Vijay definiram “a inteligência artificial [como] o estudo de ideias para criar máquinas que respondam a estímulos consistentes com as respostas tradicionais dos humanos, dada a capacidade humana de contemplação, julgamento e intenção.” (Shubhendu e Vijay, 2013, p. 28) Os autores consideram que a IA é um ramo da ciência computacional dedicado à criação de máquinas detentoras de formas de inteligência que as permitem aprender novos conceitos e tarefas, bem como raciocinar e extrair conclusões acerca do mundo (Shubhendu e Vijay, 2013).

O sistema IA pode operar numa base de aprendizagem supervisionada ou não supervisionada. O sistema de IA numa base de aprendizagem supervisionada pode ser “definido pela utilização de conjuntos de dados rotulados, [que] são concebidos de modo a treinar ou "supervisionar" os algoritmos para classificar dados ou prever resultados com exatidão.” (IBM, 2021) Por seu turno, o sistema de IA numa base de aprendizagem não supervisionada predica o seu funcionamento no uso de algoritmos capazes de “analisar e agrupar conjuntos de dados dispersos; estes algoritmos descobrem padrões ocultos nos dados sem necessidade de intervenção humana.” (IBM, 2021)

A IA pode ser aplicada a inúmeros campos, tais como nas comunicações, na educação, nas finanças, nos transportes, no marketing, na aviação, na saúde ou na segurança.

3.1.1. DOMÍNIOS DA INTELIGÊNCIA ARTIFICIAL: BIG DATA, MACHINE LEARNING, DEEP LEARNING

A IA é um conceito que engloba diversos domínios de estudo e desenvolvimento dentro da ciência computacional. Cada um desses domínios tem por foco diferentes aspectos e aplicações da IA. Dentro desses domínios podemos encontrar “ML [*Machine Learning*] e DL [*Deep Learning*]” (Jakhar e Kaur, 2020, p. 132) Também muito importante mas não sendo um domínio específico da IA, é o conceito de *Big Data*.

Dada a dispersão de conceitos, relativamente ao termo *Big Data*, iremos adotar as definições recolhidas e analisadas por Morgado e Felgueiras. *Big Data* “é uma expressão abreviada para a recolha e análise de grandes conjuntos de dados com o objetivo de revelar padrões ou conhecimentos ocultos.” (Ferguson, 2017, citado por Morgado e Felgueiras, 2022, p.143) Outra conceção mais eclética considera que “*Big Data* é o ativo de informação caracterizado por um volume, velocidade e variedade tão elevados que exige tecnologia e métodos analíticos específicos para a sua transformação em valor.” (Mauro et al., 2016, citado por Morgado e Felgueiras, 2022, p.143)

A informação é uma ferramenta muito importante, essencial para a formação de políticas que se propõem ser úteis e eficazes. A informação auxilia o processo de decisão, uma vez que reduzindo a incerteza providencia o substrato para a informada tomada de decisão. A partir da recolha e análise de dados é possível prever as necessidades e formular as estratégias para supri-las, e desse modo otimizar a afetação de recursos.

Big Data é um conceito que reflete e engloba o processo de recolha e processamento de um grande volume de informação de modo a extrair informação útil. Esse processo é muito útil; um grande volume de dados verdadeiros, proveniente de variadas fontes e de diversos setores, organizado e referenciado, que seja organizado e analisado com rapidez torna-se útil (e não material obsoleto e candidato a arquivo).

A partir dos dados recolhidos é possível avançar para o uso do “principal elemento para a seleção e o tratamento dos dados, a fim de garantir qualidade perante a sobrecarga, diversidade e o nível não estruturado dos dados na Internet das coisas” (Morgado e Felgueiras, 2022, p. 145) - o algoritmo.

Machine Learning é “um subconjunto da IA, que inclui todas as abordagens que permitem que as máquinas aprendam a partir de dados sem que sejam explicitamente programadas.” (Jakhar e Kaur, 2020, p.132) A base do sistema de *Machine Learning* é “que o computador se torne mais inteligente sozinho, ou seja, a aquisição e descoberta automática de conhecimentos a partir de dados e da experiência.” (Munakata, 2007, p. 97)

O objetivo do processo de *Machine Learning* é utilizar algoritmos de aprendizagem automática para analisar dados. Ao tirar partido da aprendizagem automática, a eficiência de uma tarefa que envolva grandes quantidades de dados é aumentada uma vez que a aprendizagem sequencial do sistema não requer a necessidade de intervenção humana manual.

Para que a AI tenha a possibilidade de extrair os benefícios do *Machine Learning* e que o algoritmo possua a capacidade de aprendizagem automática é necessário ainda mais um substrato, nomeadamente *Deep Learning*. *Deep learning* “incorpora modelos e algoritmos computacionais que imitam a arquitetura das redes neuronais biológicas no cérebro.”(Jakhar e Kaur, 2020, p.132) O termo *deep* refere-se ao número de camadas de redes neuronais artificiais (*artificial neural networks* o termo original (ANNs)) de um sistema, que se divide em 3 camadas: a camada de entrada, que recebe os dados, a camada de saída, que produz o resultado do processamento dos dados e a camada oculta, aquela que extrai os padrões dos dados. (Jakhar e Kaur, 2020)

3.2. SMART CITY: RURAL VS URBANO, SMART CITY

Para o estudo da prevenção de incividades, devemos focar o estudo no local onde este fenómeno é mais comum: o espaço urbano. Para tal torna-se útil estabelecer a diferença entre dois conceitos: rural e urbano.

Pateman (2011) oferece-nos um conjunto de marcadores chave úteis para a diferenciação de agrupamentos populacionais, nomeadamente a dimensão populacional, a concentração populacional e a distância entre aldeamentos. Estes indicadores são de carácter geral ainda assim permitem estabelecer diferenças entre diferentes agrupamentos populacionais. Utilizando marcadores de carácter menos generalista, Scott et al. (2007) identificam 5 dimensões identificativas do espaço rural, nomeadamente a baixa densidade populacional, o uso extensivo da terra, a predominância do setor primário tanto na economia como no emprego, a coesão social e governativa e ainda dimensão oposta que estas dimensões aportam comparativamente ao espaço urbano.

A partir destas dimensões podemos caracterizar o espaço urbano por acolher sobretudo atividades económicas do setor secundário e terciário, por acolher mais residentes por metro quadrado, por oferecer melhores acessibilidades e acesso à informação e serviços. Por oposição, o contexto rural é caracterizado por albergar primariamente atividades económicas do setor primário, por acolher menos residentes por metro quadrado, por dispor os serviços e infraestruturas mais espalhados pelo território e consequentemente por oferecer menor acessibilidade aos seus habitantes.

No contexto português, a unidade administrativa de base é a freguesia. Com vista à criação de indicadores caracterizadores do espaço urbano foi celebrado um protocolo entre o Instituto Nacional de Estatística e a Comissão de Coordenação da Região de Lisboa e Vale do Tejo. A partir desse protocolo (Monteiro, 2000) foram definidas três tipologias de freguesia: freguesia urbana, freguesia semiurbana e freguesia rural. As freguesias urbanas podem assim ser consideradas caso “possuam densidade populacional superior a 500 Hab./Km² ou que integrem um Lugar com população residente superior ou igual a 5000 habitantes” (Monteiro, 2000, p.3) As freguesias semiurbanas podem assim ser consideradas caso “possuam densidade populacional superior a 100 Hab./Km² e inferior ou igual a 500 Hab./Km²” (Monteiro, 2000, p.3) ou ainda caso “integrem um Lugar com população residente superior ou igual a 2000 habitantes e inferior a 5000 habitantes.” (Monteiro, 2000, p.3) Quanto às freguesias rurais, podem ser enquadradas nessa categoria todas as que não se enquadrem nas tipologias urbano ou semiurbano.

De modo a adequar-se tanto a fins estatísticos como para fins de planeamento, a discriminação entre diferentes áreas geográficas foi refinada utilizando os seguintes fatores: a freguesia é a unidade geográfica de análise, a área urbana é definida a nível de concelho, as freguesias

que integram uma área urbana têm de apresentar contiguidade espacial, a classificação estatística- freguesias urbanas, semiurbanas e rurais- é o suporte da estrutura de definição das área urbana e a freguesia sede de concelho não é integrada em Áreas Predominantemente Rurais. A partir destes fatores o Instituto Nacional de Estatística criou uma Tipologia de áreas Urbanas “composta por três níveis: Áreas predominantemente urbanas; Áreas medianamente urbanas; Áreas predominantemente rurais.” (Monteiro, 2000, p.3)

A configuração do território, as infraestruturas, a concentração populacional, a vivência da vida em comunidade é diferente. Devido a estes fatores também as manifestações de violência são diferentes nas áreas predominantemente urbanas, nas áreas medianamente urbanas e nas áreas predominantemente rurais.

O crescimento das cidades resulta também no crescimento dos problemas naturalmente associados a grandes aglomerados populacionais, como o aumento de fenómenos que provocam a degradação do meio ambiente e a diminuição da qualidade de vida. A poluição, seja sonora, atmosférica, visual, o congestionamento no trânsito, a violência ou as incivildades têm o potencial de se acumularem em contexto urbano, especialmente em contexto densamente povoado.

Paralelamente ao fenómeno da urbanização, o desenvolvimento tecnológico acelerou e procurou oferecer solução a esses desafios. Surgiu um novo tipo de cidade, essas cidades “que utilizam as TIC [Tecnologias de Informação e Comunicação] para resolver problemas urbanos são frequentemente designadas por "*Smart city*.” (Laufs, 2022, p.45)

O termo *Smart City* ou cidade inteligente está em voga, tão amplamente é empregue que pode significar quase tudo e nada ao mesmo tempo. Um nevoeiro conceptual que é causado pelas diferentes valências que podem ser utilizadas como marco identificador e característico do conceito. As diferentes possibilidades de classificar a inteligência de uma cidade podem ser “(i) de base tecnológica, (ii) de base no domínio, (iii) de base na integração e (iv) de base em dados.” (Maggioni, 2021, p. 86)

Com base em Maggioni (Maggioni, 2021) exemplificamos cada um dos grupos:

i) Os conceitos baseados em aspetos tecnológicos consideram que é a utilização articulada de software, hardware, tecnologias de rede, sensores e algoritmos que define a *Smart City*.

ii) os conceitos assentes na base de domínio (*domain-base* sendo o termo original) afirmam que há determinados setores, onde a interação entre o capital social e humano com as tecnologias de informação gera setores inteligentes dentro de uma estrutura urbana.

iii) as definições baseadas na integração interpretam que a cidade só é inteligente se houver interligação entre todos os sistemas tecnológicos utilizados pelo município.

iv) as definições que fundamentam a inteligência de uma cidade na utilização de dados, concedem o seu foco ao processo de recolha, gestão, transmissão, segurança e utilização da informação recolhida do meio.

Para além dos diferentes grupos de conceitos enumerados, existem ainda conceitos de *Smart City* que incluem aspetos sociais relacionados com a sustentabilidade e qualidade de vida dos cidadãos ou ainda os aspetos de governação participativa como elementos característicos da cidade inteligente.

Ramaprasad et al. navegaram esse nevoeiro no ano de 2016, (Ramaprasad et al., 2017) efetuando uma pesquisa em inglês no Scopus, uma das maiores base de artigos académicos, pelo termo “*Smart City*” presente no título, resumo ou palavras-chave de artigos académicos. Após seleção, foi possível apurar a existência de 373 artigos científicos. Depois de analisar o universo de conceitos, os autores (Ramaprasad et al., 2017) avançaram uma definição de *Smart City* que representa uma construção composta por duas partes, cada uma das quais é uma construção complexa: $Smart\ City = f(Smart + City)$, sendo que $Smart = f(Structure + Function + Focus + Semiotics)$ e $City = f(Stakeholders + Outcome)$. E os termos *Smart + City* contêm subelementos descritivos.

Desconstruindo a terminologia e preservando a língua original, poderíamos definir a cidade inteligente como (Ramaprasad et al., 2017): $f(Smart + City) \Leftrightarrow f((Structure \subset [Architecture, Infrastructure, Systems, Services, Policies, Processes, Personnel]) + (Functions \subset [Sense, Monitor, Process, Translate, Communicate]) + (Focus \subset [Cultural, Economic, Demographic, Environmental, Political, Social, Technological, Infrastructural]) + (Semiotics \subset [Data, Information, Knowledge])) + ((Stakeholders \subset [Citizens, Professionals, Communities, Institutions, Businesses, Governments]) + (Outcomes \subset [Sustainability, Quality of Life, Equity, Livability, Resilience]))$

A *Smart City* pode, através da utilização da Internet das Coisas, diagnosticar, prever riscos e assegurar uma resposta adequada. A *Smart City* centra-se na exploração das potencialidades proporcionadas pelas novas tecnologias, centra-se no emprego de inovadoras estratégias de gestão, na utilização eficaz dos recursos; o seu objetivo é potenciar o tecido urbano, criar sinergias entre as dimensões macro e micro do sistema.

4. ADMINISTRAÇÃO PÚBLICA

Administrar, do latim *administratio*, significa dirigir superiormente um organismo. A administração pode ter como alvo tanto organismos públicos como privados, no âmbito desta investigação vamos focar-nos na administração da *res pública*.

A CRP é a primeira e principal fonte de direito do ordenamento jurídico, pelo que qualquer lei hierarquicamente inferior não pode dispor contra as normas nela dispostas. Para garantir a execução dos princípios consagrados constitucionalmente surge o Direito Administrativo. É este que por sua vez orienta a Administração Pública na prossecução do interesse público e na prestação de serviços aos cidadãos.

A Administração Pública (AP), como organismo, tem as seguintes características (Paludo, 2010): é executora, é instrumental, tem competência limitada, possui responsabilidade técnica, possui poder administrativo, é dependente e tem natureza neutral e possui hierarquia.

A AP é executora pois tendo por objetivo a prossecução do interesse público e a prestação de serviços aos cidadãos, “presta serviços públicos e pratica atos administrativos através dos seus órgãos e agentes.” (Paludo, 2010, p.23) A sua vertente instrumental advém do facto de esta ser o meio através do qual o Estado e o Governo promovem o desenvolvimento da sociedade, sendo que cada organismo tem competência limitada por legislação que “fixa os limites da atuação administrativa.” (Paludo, 2010, p.23)

A Administração Pública tem poder administrativo, ou seja, “as suas decisões se restringem a assuntos técnicos, financeiros e jurídicos” (Paludo, 2010, p.23); essa atuação deve obedecer preceitos jurídicos e técnicos sob pena da nulidade de atos que não obedeçam às

normas e também por tal consideramos que a Administração Pública tem responsabilidade técnica. “A sua função consiste em implementar as decisões tomadas pelo Governo, pelo Legislativo ou pelo Judiciário,” (Paludo, 2010, p.24) a sua natureza é dependente e neutral. E naturalmente, como qualquer estrutura não afetiva que envolva mais que três elementos, a AP é uma estrutura hierarquizada na qual existe a subordinação dos órgãos inferiores aos órgãos superiores.

A Administração Pública pode ser compreendida em duplo sentido: sentido orgânico e sentido material.

Em sentido orgânico a Administração Pública pode ser definida como,

O conjunto de órgãos, serviços e agentes do Estado e demais organizações públicas que asseguram, em nome da coletividade, a satisfação disciplinada, regular e contínua das necessidades coletivas de segurança, cultura e bem-estar. (Caupers, 2007, p.37).

E em sentido material ou funcional a Administração Pública pode ser definida como

O conjunto de acções e operações desenvolvidas pelos órgãos, serviços e agentes do Estado e demais organizações públicas ocupados em assegurar, em nome da colectividade, a satisfação disciplinada, regular e contínua das necessidades colectivas de segurança, cultura e bem-estar. (Caupers, 2007 p.38).

4.1. POLÍTICAS PÚBLICAS

Cabe ao Governo a função de programar as orientações político-estratégicas da *res pública*, ou seja, cabe ao órgão executivo definir, em conjunto com diversos organismos, a definição das políticas públicas.

Não sendo consensual na comunidade científica a definição daquilo que consiste a política pública, apresentaremos vários conceitos.

A definição mais difundida considera por “política pública é tudo que os governos escolhem fazer ou não fazer” (Dye, 1975, p.1). Também em termos mais elaborados Paludo define políticas públicas como

Um conjunto de processos, decisões e ações quanto a alocação de recursos, que congregam diferentes atores e concentram esforços, utilizados pelos governos com vistas a mudar uma realidade, promover o desenvolvimento, efetivar direitos e atender necessidades público-sociais. (Paludo, 2021, p. 225)

Muito semelhantemente define Cardim, que considera

Políticas públicas as decisões tomadas pelo governo, destinadas à resolução de problemas que afectam a sociedade ou à introdução de regras e orientações que determinam o modo de funcionamento do colectivo dos cidadãos e das instituições e actores que operam na sua esfera de actuação. (Cardim, 2007, p.144)

Já Aguiar (1989) define política pública como um programa de ação próprio de organismo públicos ou governamentais que visando solucionar um problema estabelece um conjunto de normas coercitivas tendentes a atingir determinados objetivos.

Sumariamente podemos considerar as políticas públicas os processos, decisões e ações (ou inações) dos governos, destinadas à resolução de problemas, à introdução de orientações que determinam o modo de funcionamento do coletivo e à promoção do desenvolvimento.

4.2. POLÍTICAS DE SEGURANÇA

Relativamente à segurança, mais precisamente ao fenómeno da criminalidade, existe um conjunto específico de políticas que têm por objetivo combater ameaças à segurança pública-as políticas de segurança. Prever e gerir a segurança é a sua função. “As políticas de segurança são tudo aquilo que constitui matéria de opção do governo, seja ato ou omissão que decorre no exercício da sua atividade.” (Clemente, 2013, p. 35)

Tendo por foco a vertente interna da segurança (Sousa, 2023) considera que a política de segurança interna, da responsabilidade do Governo, visa salvaguardar a ordem e a segurança públicas contra perigos provenientes do interior e que a mesma consiste no conjunto de princípios, orientações e medidas tendentes a garantir a segurança.

Devemos referir que o termo políticas de segurança retrata um universo muito vasto e cuja abrangência ultrapassa o objeto da presente investigação, pelo que nos cingiremos ao contexto urbano. Com o foco no contexto urbano, as políticas de segurança urbana são programas concebidos por administradores locais para prevenir e combater fenómenos de incivilidade, criminalidade e insegurança no contexto da cidade.

No contexto português, conforme avança Fonseca (2010) para colmatar a ausência de uma estratégia geral em termos do Sistema de Segurança Interna seria importante Portugal dispor de um Conceito Estratégico de Segurança Interna, à semelhança do que acontece com o Conceito Estratégico de Defesa Nacional, previsto na Lei de Defesa Nacional e das Forças Armadas.

5. CRIMINALIDADE EM PORTUGAL

Portugal é um dos países mais seguros e pacíficos do mundo (Institute for Economics & Peace, 2023), ocupando o 6º lugar na escala mundial. A posição é de saudar e louvável, contudo a segurança representa um dos pilares que assegura o normal funcionamento de um Estado pelo que esta deve ser um central da agenda política de qualquer Governo. A realidade pacífica portuguesa insere-se num contexto global e europeu marcado pela incerteza e pela instabilidade.

O Relatório Anual de Segurança Interna (IASI) evidencia os principais fenómenos violentos internacionais que podem afligir o espaço português. No ano de 2023 (Relatório Anual de Segurança Interna, 2023) apontou diversos fenómenos que ameaçam a segurança interna, nomeadamente a cibercriminalidade, a ameaça terrorista de matriz islamista, as atividades políticas de extrema-direita e de extrema-esquerda, as atividades extremistas ambientalistas, o tráfico de estupefacientes, o tráfico de armas, a imigração ilegal e o branqueamento de

capitais. De entre os fenómenos apontados, a cibercriminalidade assumiu posição destacada; a delinquência em ambiente digital, na forma de *hacktivismo*, procurando desestabilizar a segurança e a sociedade democrática, a cibercriminalidade internacional altamente organizada que leva a cabo ações de cifragem e sequestro ou simplesmente a ação direta ou indireta de Estados que cometem ataques cibernéticos.

Tendo-se mantido relativamente estável entre 2014 a 2019, ao longo dos últimos três anos, Portugal tem registado um aumento da criminalidade que já ultrapassou o nível de criminalidade reportada em 2014.

Em 2022 foram reportadas 343.845 participações, em 2023 o número total de participações criminais registadas pelos Órgãos de Polícia Criminal- a Guarda Nacional Republicana, a Polícia de Segurança Pública, a Polícia Judiciária, o Serviço de Estrangeiros e Fronteiras, a Polícia Marítima, a Autoridade de Segurança Alimentar e Económica, a Autoridade Tributária e Aduaneira e a Polícia Judiciária Militar - foi de 371.995. Tal equivale ao aumento de 28.150 participações e a uma variação de +8,2% em relação ao ano de 2022.

Em termos de distribuição geográfica, os distritos de Lisboa, Porto e Setúbal representam 48% das participações. (Relatório Anual de Segurança Interna, 2023) Lisboa é o distrito português mais criminógeno e em termos de distribuição municipal, segundo o Pordata (Pordata, 2023), Lisboa é o município com mais crimes registados pelas polícias, seguido pelo Porto e por Sintra.

Com exceção do distrito de Coimbra, em todos os distritos de Portugal continental e insular, a criminalidade reportada aumentou face ao ano de 2022.

Dentro da criminalidade reportada, os crimes contra o património representam 51% do total de participações. Juntamente com os crimes contra as pessoas e os crimes contra a vida em sociedade, estas três categorias criminais representam a maioria da criminalidade reportada, nomeadamente 87% do total. No tocante ao ano de 2023 (Relatório Anual de Segurança Interna, 2023) salienta-se a subida, que em termos absolutos representa 18.727 participações, observada em cinco tipologias criminais: outras burlas, abuso de cartão de garantia ou de crédito, ofensa à integridade física voluntária simples, abuso de confiança fiscal e condução de veículo com taxa de álcool igual ou superior a 1,2g/l.

Em termos de descidas, verificou-se uma diminuição, que em termos absolutos representa 5.472 participações, em cinco tipologias criminais: incêndio, fogo posto em floresta, mata, arvoredo ou seara, furto em veículo motorizado, furto em residência com arrombamento, escalamento ou chaves falsas, burla informática e nas comunicações e condução perigosa de veículo rodoviário.

5.1. CRIMINALIDADE VIOLENTA

De entre a criminalidade destacamos a importância da criminalidade violenta não tanto pela expressividade estatística, mas pelo impacto que tem na vida em sociedade.

Relativamente a esta temática, conforme elucida Quaresma (2021) em Portugal, coexistem duas definições relevantes no domínio da criminalidade violenta, uma inscrita no Código de Processo Penal -de criminalidade violenta e de criminalidade especialmente violenta- e a que é utilizada em sede do RASI- criminalidade violenta e grave.

A CRP, no n.º 3 do art.º 34.º, referencia o termo criminalidade especialmente violenta, contudo nos termos do aludido artigo a natureza deste tipo de criminalidade não é clara pois o termo é aludido juntamente com um outro tipo de criminalidade, a criminalidade altamente organizada. A clarificação é-nos dada pelo Código de Processo Penal (CPP).

Tendo em consideração a heterogeneidade da realidade sobre a qual versa o processo penal, é estabelecida uma distinção entre a criminalidade grave e a pequena criminalidade, sendo explanado que são “duas realidades claramente distintas quanto à sua explicação criminológica, ao grau de danosidade social e ao alarme coletivo que provocam.” (Código de Processo Penal, 1987)

Enquadrada na criminalidade grave está a criminalidade violenta e especialmente violenta. Relativamente aos dois tipos criminais enunciados, o CPP, nas alíneas j) e l), do art.º 1.º, define criminalidade violenta como

As condutas que dolosamente se dirigirem contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou a autoridade

pública e forem puníveis com pena de prisão de máximo igual ou superior a 5 anos. (Código de Processo Penal, 1987)

Quando tais condutas se revestem de caráter especialmente doloso são categorizadas como especialmente violentas e a moldura penal eleva-se para a prisão de máximo igual ou superior a 8 anos.

O Sistema de Segurança Interna, entidade responsável pela elaboração do RASI, aglutina 26 crimes, “ 22 crimes autónomos do CP [Código Penal] e 4 crimes previstos em legislação avulsa (lei do terrorismo)” (Quaresma, 2021, p. 92) e cunha o conceito de criminalidade violenta e grave, assinalando que “ as tipologias criminais que integram a criminalidade violenta e grave têm como denominador comum a violência física ou psicológica e causam forte sentimento de insegurança.” (Relatório Anual de Segurança Interna, 2023, p.39)

A criminalidade violenta e grave inclui as seguintes tipologias criminais: homicídio voluntário consumado; ofensa à integridade física voluntária grave; rapto, sequestro e tomada de reféns; roubo por esticção; roubo na via pública exceto por esticção; roubo a residência; roubo de viatura; roubo a banco ou outro estabelecimento de crédito; roubo a tesouraria ou estações de correio; roubo a farmácias; roubo a ourivesarias; roubo em posto de abastecimento de combustível; roubo a outros edifícios comerciais ou industriais; roubo a estabelecimento de ensino; roubo em transportes públicos; outros roubos; extorsões; pirataria aérea e outros crimes contra a segurança na aviação; motim, instigação ou apologia pública do crime; associações criminosas; resistência e coação sobre funcionário; outras organizações terroristas e terrorismo internacional; organizações terroristas e terrorismo nacional. (RASI, 2023)

O RASI de 2023 reporta que o número total de participações enquadradas na criminalidade violenta e grave aumentou comparativamente a 2022, registando uma variação de +5,6%. Os crimes de roubo na via pública (exceto esticção), roubo por esticção, resistência e coação sobre funcionário e extorsão representam 75,7% da criminalidade violenta e grave.

5.2. SENTIMENTO DE INSEGURANÇA

Relacionado com a criminalidade efetiva, mas podendo ser considerada uma variável separada é o sentimento de insegurança. Isto porque enquanto a criminalidade é um conceito objetivo medido através de parâmetros factuais, como seja através de condutas tipificadas ou através de participações oficiais, o sentimento de insegurança é um conceito subjetivo, não por isso menos relevante, mas mais abstrato no tratamento, pois varia consoante a predisposição mental do sujeito em questão. Apesar de intimamente ligados, a criminalidade e o sentimento de insegurança são dois conceitos diferentes que não têm necessariamente o comportamento correlacionado.

O sentimento de insegurança é um conceito complexo porque é subjetivo, variando de acordo com as características psicológicas do sujeito, e por isso a sua medição é complexa.

Em relação à justaposição entre as desordens físicas e sociais, ou seja, incivildades e o medo do crime, Hunter (1978) refere que as incivildades físicas e interpessoais desempenham um papel importante no sentimento de insegurança pois a sua ubiquidade supera a vivência do crime. Enquanto o crime é menos experienciado, a acreção e a erosão do meio físico envolvente, como por exemplo edifícios em mau estado ou vestígios de lixo na via pública, é vivenciada por todos os membros da sociedade; a partir do ambiente físico os agentes fazem inferências acerca dos seus habitantes e da sociedade civil existente no espaço. Por esse motivo “bairros bem conservados, independentemente da classe social, transmitem uma aparência de ordem e provocam menos medo.” (Hunter, 1978, p.7)

Semelhantemente, Sebastian Roché correlaciona as incivildades e o sentimento de insegurança. Segundo o autor (Roché, 2002) o sentimento de insegurança é um sentimento pessoal de desconforto, influenciado pelas incivildades, que resulta na perceção da perda de ordem.

Na mesma linha, mas aprofundando aspetos sociológicos do problema, está Ferreira (2003) que considera que a crescente preocupação com a criminalidade e a insegurança não se deve tanto à criminalidade exceccionalmente violenta, mas sim “a uma relativa saturação de danos patrimoniais e de incivildades.” (Ferreira, 2003, p. 41) Ou seja, a insegurança, na maior parte dos casos, pode ser reconduzida para a criminalidade menos violenta e incivildades,

que perturbam a ordem pública, e menos frequentemente pode ser reconduzida para a criminalidade especialmente violenta. Relativamente à paradoxal correlação entre a diminuição da criminalidade violenta e o aumento do sentimento de insegurança, o autor refere que na origem deste fenómeno está “a aparente desagregação de uma identidade baseada em laços e solidariedades sociais tradicionais.” (Ferreira, 2003, p. 42). Os comportamentos incivilizados, ou seja, comportamentos que não respeitam as normas básicas da vida em comunidade estabelecidas pela maioria, colocam em causa os direitos e a segurança da generalidade dos membros da sociedade. A “crise de identidade urbana” é geradora de um sentimento de insegurança e as “incivilidades, sobretudo as decorrentes dos valores, atitudes ou comportamentos públicos característicos de determinadas [coletividades], começaram assim a emergir como um forte argumento da insegurança sentida ou revelada nas grandes metrópoles.” (Ferreira, 2003, p. 43)

Outra perspetiva diferente considera que “o fenómeno da insegurança compreende duas dimensões: a insegurança objetiva e a insegurança subjetiva.” (Agra et al, 2012, p.214) Segundo os autores (Agra et al., 2012) a insegurança objetiva reporta aquilo que é factual no mundo exterior, nomeadamente o crime, a vitimação e os comportamentos desviantes na sua generalidade. Diferentemente (Agra et al., 2012) a insegurança subjetiva reporta ao impacto subjetivo e intersubjetivo da dimensão objetiva no indivíduo e na comunidade e comporta três configurações: o sentimento de insegurança, a preocupação com o crime e o medo do crime.

A distribuição do medo do crime é desigual, porque as variáveis são diferentes. Este fenómeno afeta principalmente (Agra et al., 2012) quanto ao sexo as mulheres, quanto à idade os idosos e quanto à posição social os mais carenciados.

5.3. SEGURANÇA EM SMART CITIES

As cidades acolhem grandes comunidades, nesses corpos sociais a interação entre os atores é muitas vezes marcada pela impessoalidade e pelo mercantilismo. Apesar de o contexto rural não ser isento de fenómenos violentos, a cidade é o palco por excelência para a manifestação desses fenómenos. Cidades por todo o mundo são confrontadas com problemas

de segurança, nomeadamente criminalidade e desordem, que se manifestam sob diversas formas, especialmente na forma de violência urbana e de incivilidade, estas que por sua vez aumentam o sentimento de insegurança.

Para combater o complexo problema- sentimento de insegurança- é necessária a participação e a satisfação das necessidades e interesses de uma grande variedade de atores, como por exemplo as autoridades de segurança pública, os gestores e políticos responsáveis pela manutenção e gestão das cidades, os empresários e os próprios cidadãos.

Para analisar a vertente securitária de uma *Smart city*, Laufs et al. avançaram em 2020 uma tipologia da arquitetura da *Smart city* que comporta três níveis: um nível de sensores, um nível de rede/processamento e um nível final de serviço/atuador.

A distinção entre os diferentes níveis é benéfica para compreender a cidade inteligente como um sistema constituído por diversos componentes, a diferentes níveis, desde sensores individuais, a software de análise, a servidores que integram os dados e asseguram a intercomunicabilidade, a programas que asseguram a atempada utilização dos dados transformados.

O primeiro nível - sensores- “consiste nas várias unidades (frequentemente heterogéneas) de recolha de dados. Estes podem ser utilizados para medir quase tudo na paisagem urbana.” (Laufs et al., 2020, p.6) Depois de recolhidos os dados, estes migram para o segundo nível- rede/processamento- onde são armazenados e processados. O terceiro e último nível - serviço/atuador- representa a manifestação concreta que provoca a alteração física no ambiente ou presta o serviço pretendido.

Relativamente ao funcionamento do sistema e a relação entre os seus diferentes níveis, Laufs et al. constataram em 2020 três modalidades diferentes.

A primeira modalidade incorpora o uso de novas tecnologias para cumprir funções de segurança tradicionais, dentro desta modalidade podemos incorporar mecanismos que, sem a intervenção de infraestruturas de segurança mais alargadas, localmente controlam a prática de comportamentos indesejados e contêm mecanismos que identificam e autenticam o acesso de sujeitos a áreas restritas.

A segunda modalidade integra os sistemas tecnológicos com capacidade instalada e que são alvo de melhorias, nomeadamente melhoria do hardware, software e da intercomunicabilidade entre sistemas, para cumprir os desígnios da cidade inteligente.

A terceira modalidade reúne os sistemas que desempenham novas funções, sendo que as mesmas “não correspondem às funções tradicionais das intervenções de segurança.” (Laufs et al., 2020, p. 37)

Tendo por foco melhorar a segurança na cidade através da arquitetura, em 2009 Cai e Wang avançaram a proposta de produzir planos de ordenamento do território tendo em consideração os seguintes fatores: segurança psicológica, segurança comportamental, defesa da segurança e segurança contra catástrofes.

A segurança psicológica advém (Cai e Wang, 2009) de um sentimento de controlo e previsibilidade do ambiente, esse estado é alcançado através de um processo cognitivo que recorre aos estímulos ambientais para efetuar inferências.

A fim de influenciar [a ideia de] segurança psicológica das pessoas, fatores ambientais podem ser utilizados para aumentar a territorialidade, o controlo e a propriedade dos lugares espaciais, de modo a melhorar o sentimento de pertença. (Cai e Wang, 2009, p.221)

Um panorama urbano pautado pela excessiva urbanização, pela presença de edifícios antigos, pela ausência de espaços públicos de lazer, por rodovias congestionadas, por urbanizações clandestinas e insalubres e pela prática de incivildades “provocará a destruição do sentimento de ordem, impactando grandemente a interpretação da segurança psicológica.” (Cai e Wang, 2009, p.221)

A segurança comportamental no contexto da arquitetura promotora da segurança reporta para a conceção do espaço de modo a minimizar a ocorrência de acidentes derivados do uso do ambiente físico. “Alguns fatores do espaço urbano podem ferir as pessoas e mesmo pôr em perigo a sua vida quando acoplados a certos comportamentos e atividades.” (Cai e Wang, 2009, p.221) Exemplos dessas condicionantes físicas são superfícies demasiado suaves que provocam quedas quando associadas à chuva, passeios públicos desnivelados, passeios públicos que não separam a via pedestre da via rodoviária ou a iluminação insuficiente.

A defesa da segurança refere-se à “ integração do básico princípio de CPTED no desenho de fatores como a disposição arquitetónica, a forma espacial, a estrutura rodoviária e a iluminação.”(Cai e Wang , 2009, p.224) Para facilitar a gestão e manutenção das zonas urbanas, proteger os cidadãos, aumentar a possibilidade de identificar, prevenir e intervir prontamente contra a criminalidade e os atentados terroristas, devem ser incluídos no traçado arquitetónico componentes que tornem o espaço defensável.

A segurança contra catástrofes reveste grande importância no contexto cidadão pois “a densa urbanização terá sempre um efeito amplificador e cumulativo no grau de dano das catástrofes naturais.” (Cai e Wang, 2009, p.224) As cidades resilientes são incentivadas a implementar políticas e medidas que contribuam para o aumento da resiliência e a redução dos riscos associados a catástrofes naturais.

Para a gestão otimizada e holística dos recursos que visam debelar as situações que ameaçam a qualidade de vida dos cidadãos é necessário agregar os diferentes domínios e para tal a tecnologia otimiza o processo.

5.4. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES

As atividades de investigação e desenvolvimento contribuem para aprofundar e progredir o conhecimento científico. O trabalho investigativo e criativo, conduzido de forma sistemática com o objetivo de aumentar o conhecimento, deve ser aplicado à realidade por forma a aumentar a sabedoria humana e melhorar a qualidade de vida. A segurança não é imune ao progresso da ciência e da tecnologia; a ciência aplicada à segurança- pública e privada- transforma o modo de operação do setor introduzindo novas ferramentas para combater o crime e as incivildades. Ferramentas hodiernamente consideradas vulgares, como o rádio bidirecional, o automóvel e o telefone, despoletaram uma mudança substancial no modo de funcionamento das organizações policiais. (Anderez et al., 2021)

Na senda de analisar as inovações tecnológicas aplicadas na prevenção da criminalidade em geral e do controlo da criminalidade por parte da polícia, em 2011 Bryrne e Marx avançaram

uma tipologia bipartida: tecnologia baseada em equipamentos e tecnologia baseada na informação.

Tecnologia baseada em equipamentos “inclui novos materiais, dispositivos e equipamentos que podem ser utilizados para cometer crimes ou para prevenir e controlar a criminalidade.” (Bryrne e Marx, 2011, p.19) Por seu turno tecnologia baseada na informação inclui “novos programas informáticos, sistemas de classificação, técnicas de análise criminal e técnicas de partilha de dados/integração de sistemas” (Bryrne e Marx, 2011, p.19) e envolve a “utilização estratégica da informação para prevenir a criminalidade.” (Bryrne e Marx, 2011, p.19)

Tendo em consideração a tipologia apresentada, focar-nos-emos na presente investigação no uso dos sistemas de CCTV conjugando tanto a vertente da tecnologia baseada em equipamentos como a vertente da tecnologia baseada na informação.

Embora o uso do CCTV na cidade inteligente possa ser aplicado em diversas áreas, mais precisamente na área da saúde, onde pode ser utilizado para controlar idosos, situações pandémicas ou calamitosas ou ainda oferecer serviços de telemedicina, na área da gestão rodoviária, onde o CCTV pode ser utilizado para otimizar o fluxo de tráfego, gerir parqueamentos ou detetar incidentes na rodovia, na área ambiental onde as câmaras podem ser utilizadas para monitorizar o tempo, fogos ou fumos, (Myagmar-Ochir e Kim, 2023) presentemente o foco será a utilização do CCTV na área da segurança pública, onde esta tecnologia pode ser utilizada para monitorizar o espaço público por forma a detetar precocemente a atividade criminal e a prática de incividades.

5.4.1. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES: CRÍTICAS

A utilização destes sistemas não é isenta de desaprovação, mormente relacionada com a ingerência do Estado na privacidade individual. Proponentes que repudiam a utilização de câmaras de monitorização “entendem o crescimento do CCTV como uma intrusão, com visões de um "*Big Brother*" orwelliano a invadir a privacidade pessoal.” (Ratcliffe, 2021, p. 6) Tal visão resulta do entendimento que a recolha de imagens de um sujeito sem a sua

expressa e consentida aprovação constitui um atentado ao direito de privacidade e o direito à reserva da intimidade da vida privada.

Conforme a interpretação do Acórdão nº 16/15.2GEVCT.G (2016), o direito à imagem consiste no direito de a pessoa poder escolher ou recusar ser fotografada ou filmada bem com permitir ou recusar que o seu retrato seja exposto em público, por se considerar que a imagem é um reflexo da sua identidade pessoal. Logo, para que a captação de imagens seja legal é necessário haver o consentimento do visado.

Por outro lado, o direito de reserva da intimidade da vida privada reporta-se,

[Ao] direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. (Canotilho e Moreira, 2007, p. 467).

Por conseguinte a captura de imagens e vídeos em espaços públicos pode constituir na devassa da vida privada na medida em que podem ser registados momentos que o indivíduo prefira manter privados.

No que respeita a possíveis efeitos secundários da instalação e operacionalização dos sistemas de CCTV, são reportadas diversas consequências, nomeadamente o deslocamento do crime para áreas não vigiadas, o aumento da suspeita ou do receio de crime e o aumento das denúncias de crimes. (Ratcliffe, 2021)

Conscientes da monitorização do espaço, os perpetradores podem alterar a sua forma de operar, isto é, alterar a forma como cometem o crime ou podem alterar o local em que operam. O fenómeno que pode suceder é o seguinte: “em vez de uma redução das infrações, é possível que os infratores reajam deslocando as suas infrações para um local fora da vista das câmaras CCTV.” (Ratcliffe, 2021, p.14)

Também conscientes da monitorização, parte dos cidadãos consideram que o objetivo do CCTV é espiar os indivíduos. Em razão desse entendimento, a instalação de sistemas de CCTV gera um estado de desconfiança que interfere no bem-estar de uma parte dos cidadãos.

Reconhecemos que existe a possibilidade de estes sistemas representarem uma ameaça à liberdade do cidadão quando o intuito que leva à sua instalação não se cinge à proteção e

promoção dos direitos, liberdades e garantias, mas sim para o controlo da vida do cidadão e para a espionagem doméstica.

O epítome da utilização dos sistemas CCTV para controlar, em escala micro e individualizada, o cidadão pode ser encontrado na República Popular da China. A cidade de Shentzen, na República Popular da China, testou um sistema de CCTV com a capacidade de alertar a polícia quando um número excessivo de indivíduos se aglomera num local (Ratcliffe, 2021). Adicionalmente à capacidade de deteção de aglomerações, “foi desenvolvido um programa que utiliza a base de dados de identificação nacional da China e um software de reconhecimento facial que permitirá à polícia identificar indivíduos sob videovigilância.” (Ratcliffe, 2021, p.21)

Contudo o enquadramento político e legal é diametralmente oposto entre a República Popular da China e a generalidade dos Estados Ocidentais e pelo tanto o enquadramento que rege a videovigilância é necessariamente diferente.

Uma outra eventual consequência negativa gerada pela instalação de câmaras de monitorização pode ser o aumento da criminalidade reportada de determinados tipos de criminalidade pois “muitas infrações têm taxas de participação baixas, especialmente atos de violência de menor gravidade, grafiti e infrações relacionadas com estupefacientes.” (Ratcliffe, 2021, p.15) O aumento da criminalidade reportada pode dever-se a dois fenómenos diferentes. Primeiramente pode resultar do facto de a atividade criminal ser detetada em flagrante delito por operadores, que transmitem essa informação às unidades que são responsáveis por efetuar o acompanhamento da situação e formalizar a participação. E secundamente pode resultar da denúncia por parte dos cidadãos de atos criminosos que os mesmos acreditam ter sido captados pelos dispositivos de captação de imagem e gravados.

Quanto à operacionalização dos meios, relativamente aos sistemas de videovigilância pode ser apontada crítica à componente humana. Tendo em conta que existem limitações em termos de meios, humanos e temporais, para monitorizar a área abrangida pelos dispositivos de captação de imagem, é necessário racionalizar a tática de intervenção de modo a maximizar a sua eficácia pois “o grande volume de informação recebe um sistema de CCTV ameaça sobrecarregar os operadores com excesso de informação.”(Norris e Wilson, 2017, p. 158) Para maximizar a eficácia torna-se recomendado a monitorização aproximada de comportamento suspeito e a ignorar comportamento rotineiro, essa tática pode gerar

procedimentos enviesados. Ora aquilo que pode ser categorizado como comportamento suspeito não é objeto de análise objetiva sendo assim definido com base no senso comum. O operador que monitoriza estes sistemas pode selecionar pessoas de interesse com base em conceitos preconcebidos que originam uma sobre vigilância de determinados grupos.

Questionando aquilo em que consiste o senso comum do comportamento suspeito e partindo da questão:

Perante uma avalanche de imagens e uma gama limitada de dados sensoriais, como é que o operador de CCTV filtra seletivamente [as] imagens para decidir o que merece uma atenção mais detalhada? (Norris e Wilson, 2017, p. 160).

Após a análise de 592 horas de monitorização de três centros urbanos, em 1996 Norris e Wilson constataram que o alvo de monitorização aproximada é de sexo masculino, é um jovem adulto e é caucasiano. Os indivíduos de sexo masculino, embora representando cerca de metade da população, representam 93% das pessoas de interesse, comparativamente aos indivíduos de sexo feminino que contabilizaram apenas 7% das pessoas de interesse monitoradas pelos operadores de CCTV. Os indivíduos de sexo feminino são “quase invisíveis para as câmaras” (Norris e Wilson, 2017, p. 172), sendo que são alvo de monitorização sobretudo quando há histórico da prática de furtos em estabelecimentos comerciais ou quando as mesmas estão envolvidas em desacatos. Relativamente à faixa etária, a juventude é o foco do operador de CCTV, mais precisamente “os adolescentes - que representam menos de 20% da população - foram objeto de 40% das vigilâncias direcionadas.” (Norris e Wilson, 2017, p. 162) E não toda a juventude; para direcionar a monitorização são utilizadas pistas visuais, nomeadamente a indumentária e a postura são utilizadas para fazer inferências acerca da propensão para a prática criminal e desse modo selecionar indivíduos. “Os jovens do sexo masculino, sobretudo se forem negroides ou estereotipadamente associados à classe baixa, representam o maná nos sistemas CCTV.” (Norris e Wilson, 2017, p. 172)

5.4.2. CCTV APLICADO NA PREVENÇÃO DE INCIVILIDADES: BENEFÍCIOS

A par dos possíveis malefícios derivados da instalação de sistemas de CCTV, estão também associados benefícios.

Nas palavras de Ratcliffe (2021) as câmaras de videovigilância não representam uma barreira física, não impedem o acesso a determinadas áreas, não tornam um objeto mais custoso de roubar nem tornam uma pessoa mais difícil de assaltar e roubar; representam uma forma de prevenção situacional do crime pois o delinquente, como agente racional, ao reconhecer o dispositivo infere que o risco associado à prática criminal aumenta (e conseqüentemente o risco de captura) e em razão disso coíbe-se da prática criminal. Adicionalmente ao fator acima apresentado, o autor (Ratcliffe, 2021) apresenta causas adicionais que favorecem à redução da criminalidade nos locais onde estão instalados sistemas de CCTV, nomeadamente a redução da criminalidade através da deteção e interpelação de infratores, através do melhoramento cívico aportado pelo investimento público no local de instalação e também pela mudança de comportamento de potenciais vítimas.

Num sistema de videovigilância no qual a vigilância é passiva, a informação recolhida pelos sensores pode ser muito útil para subsequente utilização no contexto investigativo pois permite a visualização de quem pratica o crime e facilita o estudo do *modus operandi* dos agentes de crimes. (Fróis, 2011) Contudo uma vez que a interpretação da informação recebida não é efetuada no momento da captação ou nos breves momentos posteriores à captação, tem pouco potencial para frustrar a prática da criminalidade pois a essência da prevenção reside na prontidão de atuação.

Somando à eventual diminuição da criminalidade, a instalação de sistemas de CCTV pode gerar uma série de outros benefícios, englobando, entre outros, a redução do sentimento de insegurança e a produção de informação com potencial para auxiliar inquéritos. (Ratcliffe, 2021)

Aludiremos a considerações acerca dos sistemas de videovigilância e avançaremos para a análise estatística do desempenho real destes sistemas. Tendo em consideração que existe

uma grande variação entre diferentes estudos “não só na metodologia, mas também nas medidas de resultados e nas variáveis independentes” (Ratcliffe et al., 2009, p. 747) explanaremos os resultados de vários estudos, sendo que anunciaremos primeiramente os critérios metodológicos e secundamente os resultados obtidos.

A revisão do estado da arte efetuada por Piza et al. em 2019 parece-nos muito pertinente para auxiliar o desenvolvimento do tema desenvolvido no presente estudo. Sublinhando a temática do impacto do CCTV na prevenção da criminalidade, os autores procederam à revisão sistemática dos artigos publicados e procederam à metaanálise dos mesmos. A inclusão de artigos no estudo dos autores foi operada seguindo os seguintes critérios: 1) o principal objeto de estudo da intervenção deve ser o CCTV, essa relevância foi determinada em função da importância conferida diretamente pelo autor do artigo ou através da importância atribuída implicitamente em relação a diferente tópico num dado artigo; 2) a avaliação utilizou uma *outcome measure* (medida do resultado em tradução livre) resultado da criminalidade; 3) o projeto de investigação deve envolver a utilização, no mínimo, de dados da criminalidade relativamente ao período pré instalação e ao período pós instalação nas zonas alvo bem como dados relativamente a zonas de controlo; 4) A criminalidade reportada na zona-alvo e na zona de controlo deve ser superior a 20 ocorrências.

A razão de chances, do termo anglo-saxónico *Odds-ratio* (OR), foi utilizada para efetuar a comparação entre a criminalidade reportada nas zonas alvo e nas zonas de controlo. Este indicador é obtido através da divisão entre a probabilidade de ocorrência de crime e a probabilidade da não ocorrência de crime. Esta variável versa a alteração proporcional da criminalidade na área de controlo em comparação com a área experimental. A razão de chances superior a 1 demonstra um efeito desejável da intervenção, ou seja, uma razão de chances de 1,25 indica uma diminuição da criminalidade em 25% na área de controlo. Inversamente a razão de chances inferior a 1 demonstra um efeito indesejável da intervenção que no presente caso indica aumento da criminalidade nas áreas de controlo.

Após revisão do estado da arte, Piza et al. em 2019 constataram que no conjunto dos estudos sobre a eficácia do CCTV na prevenção da criminalidade a razão de chances encontrava-se em 1,141 ($p < 0,001$), o que demonstra um efeito modesto, mas significativo de prevenção da criminalidade; um tal efeito encontrado tanto na análise de maior (OR = 1,205, $p < 0,001$) quanto na de menor tamanho de efeito (OR = 1,079, $p = 0,026$). Decompondo este resultado mediano, em termos das diferentes seções geográficas, os parques de estacionamento

revelaram o melhor resultado em termos de prevenção da criminalidade, segundo os autores (Piza et al., 2019) a razão de chances nos parques de estacionamento foi de 1,588 ($p = 0,027$), o que significa a redução da criminalidade em aproximadamente 37% nas zonas-alvo em comparação com as zonas de controlo. A redução da criminalidade foi transversal, sendo que o maior desvio elevou-se a 1,618 ($p < 0,018$) e o menor desvio ficou-se por 1,620 ($p = 0,024$). Continuando com a análise das diferentes secções geográficas, nos complexos habitacionais, públicos ou privados, a análise conduzida pelos autores (Piza et al., 2019) demonstrou que a implementação de sistemas CCTV para a prevenção criminal apresentou um efeito não significativo, com um OR geral de 1,028 ($p = 0,805$), tendo a amostra com menor desvio um OR de 0,992 ($p = 0,940$) e a amostra com maior desvio um OR de 1,056 ($p = 0,663$).

Avançando decompomos também o resultado mediano, em termos de diferentes tipologias criminais; após a análise sistemática (Piza et al., 2019) evidenciou-se que a instalação de CCTV está associada a reduções significativas nos crimes relacionados com estupefacientes, com um OR de 1,249 ($p = 0,044$), nos crimes contra veículos tendo-se evidenciado que apresenta um OR de 1,164 ($p = 0,030$) e nos crimes contra a propriedade apresenta um OR de 1,161 ($p = 0,021$). A par destes resultados positivos, foram revelados padrões de não redução da criminalidade violenta ou na desordem após a instalação de sistemas CCTV. (Piza et al., 2019)

De entre os estudos analisados por Piza, Welsh, Farrington e Thomas, salientamos um estudo em particular. Esse destaque foi merecido em virtude da clareza metodológica e modo conciso de apresentação de resultados. O estudo realizado por Ratcliffe et al. em 2009 utilizou áreas de controlo e áreas de estudo para medir e comparar a prática criminal considerada grave e a prática criminal enquadrável na categoria de desordem. Quanto à fonte, foram utilizados dados da criminalidade reportada (e ocorrida na via pública) entre janeiro de 2005 e agosto de 2007 no Departamento de Polícia da Filadélfia e analisadas 18 câmaras de CCTV em 10 locais na cidade de Filadélfia, nos Estados Unidos da América. Para a área de instalação de cada câmara foram designadas duas áreas: zona-alvo e zona-tampão. O local de instalação da câmara foi considerado como a zona-alvo e a área compreendida até aproximadamente 150 metros foi incluída na zona-tampão. A restante área da circunscrição policial para além dessas duas zonas foi considerada como zona de controlo.

Relativamente à criminalidade considerada grave, Ratcliffe et al. (2009) concluíram que em nenhum dos locais onde estavam instaladas câmaras, tendo em consideração a variação sazonal, ocorreu uma variação estatística significativa. Os crimes graves diminuíram ligeiramente após a implementação das câmaras, precisamente cerca de 5%.

No que respeita a prática criminal enquadrável na categoria de desordem os dados indicam que a implementação de câmaras reduziu significativamente a criminalidade de desordem nas áreas alvo. Após a implementação destes dispositivos, tendo em consideração variações temporais e sazonais, a implementação de câmaras demonstrou uma variação negativa em 10,4% da prática criminal enquadrável na categoria de desordem. (Ratcliffe et al., 2009)

No tocante à redução geral da criminalidade após a instalação do sistema CCTV, o resultado foi heterógeno, nalgumas zonas diminuiu enquanto “em metade dos locais [de instalação], a criminalidade não diminuiu na área-alvo.” (Ratcliffe et al., 2009, p.765) No que se refere ao deslocamento do crime para zonas não vigiadas, das 12 zonas, 5 demonstraram uma redução da criminalidade após a instalação de câmaras e todas as 5 zonas evidenciaram o deslocamento do crime para zonas não vigiadas.

Respeitando o contexto português, explanaremos os resultados obtidos por Carvalho em 2020. Atendendo à entrada em funcionamento do sistema CCTV no concelho da Amadora no ano de 2017 e à acessibilidade dos registos da criminalidade reportada, o autor analisou os dados registados de criminalidade na freguesia de Águas Livres, no período compreendido entre 1 de janeiro de 2015 e 31 de dezembro de 2019. De entre as diferentes freguesias do concelho da Amadora, o autor selecionou como área de estudo a freguesia de Águas Livres tendo em consideração que “apesar de ser a freguesia com menor área, regista o maior índice de criminalidade, a maior densidade populacional e a maior concentração de câmaras de videovigilância.” (Carvalho, 2020, p. 44)

Em termos brutos, em 2020 Carvalho constatou que foram participados 6252 crimes, 3263 destes participados antes da entrada em funcionamento do CCTV e 2989 após a entrada em funcionamento do CCTV, em termos medianos tal traduz-se na ocorrência no período antes da instalação de CCTV de uma média 3,8 crimes por dia, enquanto no período de funcionamento do CCTV a média desceu para 3,1 crimes por dia, criminalidade esta que diminuiu tanto em arruamentos com CCTV como em arruamentos sem CCTV.

Comparando os dados da criminalidade registada freguesia de Águas-livres pela Polícia de Segurança Pública da Divisão Policial da Amadora com o cenário geral estatístico de Portugal reportado pelo RASI no ano de 2018, “a criminalidade registada em Águas Livres apresentou uma diminuição de 18,3% face a 2017, enquanto que a criminalidade em Portugal desceu apenas 2,6%.”(Carvalho, 2020, p. 50) Relativamente à criminalidade contra o património participada em Águas Livres, em linha com os resultados apresentados por Piza et al. em 2019, de acordo com Carvalho (2020) sofreu uma redução em termos percentuais de 25%, que em números brutos equivale à redução de 708 participações para 534 participações. Enquanto foi verificado esse decréscimo acentuado na freguesia de Águas Livres, no contexto nacional, “de acordo com o RASI de 2018, os crimes contra o património, em Portugal, entre 2017 e 2018 reduziram 0,3% de 170.832 em 2017 para 170.383 em 2018.” (Carvalho, 2020, p. 50)

Explicando os resultados obtidos por Carvalho em 2020, nesta freguesia a ocorrência de crimes na via pública diminuiu sensivelmente 14% após a instalação de sistemas de CCTV, de entre os quais foi registada uma diminuição considerável dos crimes contra a vida em sociedade, mais precisamente uma redução de 29%. Foi registada uma redução atenuada, mas não de somenos importância dos crimes contra o património, que registaram uma queda de 12%, contudo ocorreu um aumento dos crimes contra pessoas, nas ordem dos 3%. Os crimes contra pessoas revestem especial importância devido ao facto de a sua comissão causar substancial dano à integridade física e moral do indivíduo.

A instalação de sistemas CCTV, pela evidência estatística, não parece influenciar grandemente a prática de criminalidade grave pois não estão associados elevados decréscimos da sua prática. Para esta observação pode influenciar a diminuta amostra, ou seja, “o número de crimes na zona-alvo [pode ser] insuficiente para que a técnica [estatística] detetasse uma alteração estatisticamente significativa.”(Ratcliffe et al., 2009, p. 765) Ratcliffe indica também que existem “algumas provas qualitativas, de que os potenciais infratores que estão sob a influência do álcool ou de drogas podem não se importar ou lembrar que poderão estar a ser vigiados” (Ratcliffe, 2021, p. 10) e por isso não se coíbem à prática criminal.

Não incluído no âmbito da criminalidade violenta pelo Código de Processo Penal, o crime de roubo, em diversas modalidades, está abrangido na categoria da criminalidade violenta e grave. A criminalidade relacionada com roubo a pessoas na via pública (exceto esticção) e o

roubo por esticção revelaram uma diminuição em Águas Livres, após a implementação do sistema de CCTV, superior aos valores registados a nível nacional. Em termos estatísticos na freguesia de Águas Livres registou uma diminuição situada nos 24% de crimes de roubo na via pública (exceto esticção) e nos 51% em termos de roubo por esticção enquanto a nível nacional esses valores quedaram-se nos 9,4% nos crimes de roubo na via pública (exceto esticção) e de 18,6% nos crimes de roubo por esticção. (Carvalho, 2020)

5.5. CCTV INTELIGENTE

A mera instalação de câmaras de videovigilância não constitui um mecanismo automático para a prevenção da criminalidade, conforme concluiu a revisão do estado da arte efetuada por Piza et al. em 2019. Após a análise de 65 estudos na prevenção da criminalidade, de entre os quais 54 analisaram a performance de sistemas de CCTV que incorporavam a monitorização ativa da informação captada pela câmaras e 11 analisaram a performance de sistemas de CCTV que monitorizavam passivamente a informação captada pelas câmaras concluíram que “os sistemas de CCTV que incorporam monitorização ativa (n = 54) foram associados a uma redução significativa da criminalidade (OR = 1,172, p < .001).” (Piza et al., 2019, p. 145) Inversamente, Piza et al. em 2019 concluíram que os sistemas CCTV passivamente monitorizados revelaram resultados pouco significativos nas três meta-análises: tamanho médio do efeito (OR = 1,015, p = 0,633), tamanho mais pequeno do efeito (OR = 0,991, p = 0,804) e tamanho maior do efeito (OR = 1,036, p = 0,383).

Tal efeito na redução da criminalidade, também conjugável com a intervenção no ambiente físico, o aumento das operações policiais ou o envolvimento da comunidade no processo, deve-se à utilização de tática de monitorização ativa de câmaras “ para identificar e tratar proactivamente os incidentes de interesse.”(Piza et al., 2019, p. 149) Relativamente à questão da monitorização em tempo real e proativa das imagens captadas por câmaras de monitorização é de salientar a importância desta tática para a prevenção da criminalidade, com especial importância para a prevenção da criminalidade violenta, pois (Piza et al., 2019) a ocorrência de crimes violentos é precedida por uma janela de oportunidade que pode ser utilizada pelas forças da ordem pública para evitar o agravamento da situação.

O operador tem essencialmente duas funções quando visualiza a informação captada pelos dispositivos de captação de imagens: “a monitorização geral de várias transmissões de câmara em direto ou a procura de um evento, pessoa ou objeto específico em ficheiros de vídeo arquivados, normalmente associados a uma investigação.” (Chen et al., 2021, p. 391) A execução com sucesso dessas funções pode não suceder devido à possibilidade de acontecerem “falha[s] de perceção quando há poucas alterações visuais em longos períodos de vídeo.” (Idrees et al., 2018, p.1) Para melhorar o desempenho e aumentar a eficiência do operador dos sistemas de CCTV na prevenção da criminalidade, isto é ultrapassar o possível *profiling* que concentra o visionamento em determinados alvos ou a possível sobrecarga de informação que diminui a atenção ao detalhe, torna-se importante utilizar a IA. Entre os domínios da IA, “uma abordagem cada vez mais popular para colmatar as deficiências apresentadas nas redes de câmaras monitorizadas por humanos é o *Computer Vision*.” (Chen et al., 2021, p.391)

Computer Vision consiste na utilização de *machine learning* e *neural networks* “para ensinar computadores e sistemas a obter informação pertinente a partir de entradas visuais - e a fazer recomendações ou tomar medidas quando detetam defeitos ou problemas.” (IBM, 2021) Uma imagem é produzida a partir da descodificação numérica de cada um dos pixels que a compõem, “estes números atribuídos são a base de toda a manipulação, análise, interpretação, rotulagem e outras capacidades de *Computer Vision* de nível superior subsequentes.” (Idrees et al., 2018, p. 5) *Computer Vision*

Aplica algoritmos matemáticos a cada fotograma das imagens de CCTV com o objetivo de automatizar a deteção de eventos relacionados com o crime. Após a deteção de uma imagem de interesse como uma arma, um veículo em fuga ou um comportamento físico indicativo de crime alerta o operador de CCTV. (Piza et al., 2019, p. 151)

A Inteligência Artificial aplicada nos sistemas CCTV, na forma de *Computer Vision*, pelas forças da ordem pública atualmente é aplicável sobretudo a dois cenários específicos. Nomeadamente “as utilizações atuais mais comuns de *Computer Vision*, são as aplicações de reconhecimento facial e os leitores de matrículas.” (Idrees et al., 2018, p. 4) O *status quo* pode evoluir, pode ser expandido o uso deste tipo de tecnologia para englobar fins de prevenção criminal na via pública.

A não utilização da *Computer Vision* pelas forças da ordem pública é causada pela falta de desenvolvimento de software de *Computer Vision* concebido para suprir as necessidades das forças da ordem pública e pela ausência de ensaios no terreno que justifiquem os custos associados à atualização das redes de câmaras para as agências. (Idrees et al., 2018)

Entre os fatores apresentados, o segundo exerce mais influência para a não utilização deste tipo de tecnologia na prevenção criminal. Conforme realizado por Piza et al em 2019, dado o elevado custo associado à tecnologia, a introdução de operadores de câmaras e/ou agentes de patrulha adicionais nas operações de CCTV pode ser uma medida mais eficaz em termos de custos do que as tecnologias complementares de controlo da criminalidade. O inconveniente económico pode ser ultrapassado; mais recentemente “o acoplamento de câmaras de segurança a computadores económicos equipados com placas de processamento gráfico céleres colocou aplicações de CV ao alcance dos organismos públicos.” (Chen et al., 2021, p.391)

O seu uso pode ser expandido e em termos práticos o uso de *Computer Vision* por parte das forças da ordem pública (Idrees et al., 2018) pode recair sobre 2 categorias, a primeira compreende a necessidade de uma análise automatizada de fluxo de vídeo em tempo real de modo a identificar eventos de interesse que tenham o potencial de fazer perigar a segurança pública e a segunda compreende a necessidade de acelerar a pesquisa *post-hoc* de ficheiros de vídeo arquivados. Sobre a primeira categoria, a definição daquilo que consiste a normalidade, ou por outras palavras, estabelecer a diferença entre eventos de interesse que tenham o potencial de fazer perigar a segurança pública e eventos ordinários não é uma tarefa linear, por diversos motivos.

Idrees et al. (2019) apresentam três motivos explicativos da dificuldade em discernir a trivialidade ordinária da ilegalidade: primeiramente a definição quantitativa do padrão visual normal ou do anormal não está bem definida, secundamente o comportamento definido como normal evolui ao longo do tempo e pode mudar significativamente e terceiramente uma vez que os eventos de interesse que tenham o potencial de fazer perigar a segurança pública são menos usuais que os eventos inofensivos é difícil obter exemplos suficientes para treinar classificadores. Para ultrapassar esses impedimentos “os modelos [de deteção] de anomalias devem ser continuamente atualizados e incorporar as alterações ambientais.” (Idrees et al., 2018, p.9)

O uso de sistemas de videovigilância que empregam a IA apresenta diversas valências, segundo Myagmar-Ochir e Kim (2023) pode incorporar a classificação e reconhecimento de objetos, o seguimento de objetos, a detecção de ações humanas, a detecção de anomalias (e a gestão da segurança de dados.) Anunciaremos brevemente as valências do sistema, com particular enfoque para as valências mais significativas para a prevenção criminal, que são precisamente a identificação de objetos, a detecção de ações humanas e a detecção de anomalias. A questão da gestão da segurança de dados será aprofundada no próximo capítulo.

Conforme elucidam Myagmar-Ochir e Kim no estudo efetuado em 2023, a classificação de objetos auxilia a identificação e a localização de objetos específicos num fluxo de vídeo. O processo de classificação de objetos incorpora várias etapas, especificamente a aquisição de imagens, o pré-processamento de imagens, a extração de características e o reconhecimento de objetos; na etapa de pré-processamento da imagem são utilizados algoritmos de compressão de vídeo, redução de ruído e melhoramento de imagem, para fornecer as meta características que serão utilizadas na fase seguinte, na etapa da extração de características é efetuada a identificação de padrões na imagem e na etapa final, o reconhecimento de objetos é efetuado comparando as características extraídas com dados de objetos catalogados para identificar objetos de interesse. O reconhecimento de objetos pode ser realizado através do movimento, da forma, da cor ou da textura.

O sistema pode, após a identificação de um objeto de interesse num fluxo de vídeo, proceder ao seguimento ou acompanhamento de objetos específicos, à medida que se movem através dos fotogramas do vídeo, mesmo quando os mesmos estão parcial ou totalmente ocultos. Esse seguimento pode ser conduzido tendo em conta um ponto específico desse objeto, tendo em conta a localização estimada do objeto no fotograma seguinte ou tendo em conta a silhueta do objeto em questão. (Myagmar-Ochir e Kim, 2023)

A detecção de ações humanas, ou inglês o termo original *Human Action Detection* (HAR), é uma função essencial para a manutenção da segurança pública pois “comportamentos suspeitos ou criminosos e situações perigosas podem ser detetados com esta função.” (Myagmar-Ochir e Kim, 2023, p.17) Esta funcionalidade pode detetar comportamentos anormais ou classificar as ações dentro de um vídeo. A detecção de ações anormais centra-se na identificação de ações pouco comuns, invulgares ou potencialmente perigosas que não se enquadram no contexto de num determinado espaço. Neste âmbito é particularmente útil

a detecção de “atividades que ocorrem com pouca frequência, mas que são precursoras de atividades criminosas.” (Chen et al., 2021, p.397) Esta funcionalidade também classifica ações. “A classificação de ações com base no comportamento humano extrai características significativas dos dados de vídeo e utiliza algoritmos de aprendizagem profunda para classificar e identificar ações ou comportamentos específicos.” (Ko, T., 2014; Gowsikhaa et al., 2014, citados por Myagmar-Ochir e Kim, 2023, p.31)

Em relação ao uso de sistemas de videovigilância que empregam a IA, estes podem ser utilizados para a detecção de anomalias, esta valência “consiste em identificar acontecimentos ou comportamentos invulgares ou inesperados em imagens de vídeo captadas por câmaras de vigilância” (Myagmar-Ochir e Kim, 2023, p.18) e incorporado nesta valência destacamos a importância dos sistemas programados para detetar a presença de armas em espaços públicos.

Com a utilização deste tipo de tecnologia não se pretende substituir a componente humana mas sim que o operador humano se torne num supervisor. A tecnologia deteta anomalias, após a detecção de anomalias, o sistema informático alerta o operador humano para as situações de interesse a acompanhar.

6. VULNERABILIDADES ASSOCIADAS AO SISTEMA CCTV

A generalização do uso da tecnologia para solucionar questões relacionadas com a segurança na *Smart-City* deve ser acompanhada por dispositivos e procedimentos que assegurem a preservação e integridade tecnológica dos sistemas bem como mecanismos procedimentais e legais que assegurem a proteção da privacidade individual. É importante refletir sobre estas questões; negligenciá-las pode resultar na frustração do uso de mecanismos tecnológicos de segurança que simultaneamente promovam os direitos, liberdades e garantias dos cidadãos e promovam o cumprimento da missão das Forças e Serviços de Segurança.

6.1. VULNERABILIDADES TECNOLÓGICAS

É imperativo não descurar as questões de segurança, uma vez que a integridade e inviolabilidade do sistema informático é o garante do seu correto funcionamento. Pois “embora os sistemas de IA sejam geralmente “inteligentes”, são também “frágeis”, o que significa que podem ser facilmente ludibriados ou atacados.” (Hu et al., 2021, p. 2) Os ciberataques têm o potencial de destruir a integridade do sistema e permitir o acesso indevido a dados confidenciais.

Para evidenciar possíveis falhas de um sistema baseado na IA, passaremos à descrição de cada uma das fases por que este sistema é composto e também à descrição problemas de segurança associados a cada uma dessas fases.

Hu et al. (2021) indicam que o ciclo de vida de um sistema de IA pode ser geralmente dividido em cinco fases e cada uma dessas fases é vulnerável a diferentes conjuntos de ameaças à segurança. As fases que os autores avançam são as seguintes: “recolha de dados, pré-processamento de dados, formação de modelos, inferências do modelo e integração do sistema.” (Hu et al., 2021, p.3)

Na primeira fase- fase de recolha de dados- os riscos de segurança estão relacionados com o meio de recolha de dados, que podem ser subdivididos em dois métodos de recolha de dados: recolha baseada em software e recolha baseada em hardware. Hu et al. (2021) indicam que a recolha de dados baseada em software consiste na recolha, através de coletores de dados, da informação produzida pelos utilizadores quando estes utilizam a internet e que a recolha de dados baseada em hardware consiste na recolha de informação produzida em sede de equipamentos físicos. Nesta fase, os principais problemas associados estão relacionados com a integridade dos dados, mais precisamente a recolha de dados enviesados, a recolha de dados falsos, a violação dos dados e a adulteração de coletores de dados (sendo o termo original *Sensor Spoofing Attack*). Para solucionar estas questões é recomendado (Hu et al., 2021) melhorar os parâmetros que dirigem a deteção e filtragem dos dados recolhidos, proceder à verificação de proveniência, proceder à autenticação dos dispositivos coletores, investir na gestão e na formação do pessoal de modo a desenvolver os procedimentos conducentes à qualidade e segurança do processo de recolha de dados.

Na segunda fase- pré-processamento de dados- pode ocorrer a adulteração da informação original, isto porque, conforme elucidam (Hu et al., 2021) uma vez que o tamanho das imagens que software utiliza para treinar o sistema têm normalmente um tamanho fixo, por norma é necessário redimensionar as imagens de modo que correspondam ao tamanho de entrada do software. Durante esse processo de redimensionamento é necessário gerar uma nova imagem com uma resolução inferior/superior em termos de pixels do que a original, é nessa fase que hackers podem utilizar indevidamente o algoritmo, de redimensionamento para ajustar a informação ao nível dos pixels, de modo a criar uma imagem falsa. Para precaver esta vulnerabilidade recomenda-se (Kim, B., et al., 2020) a integração de um processo de deteção de imagens falsas que incorpore a redução e aumento imagem de entrada para construir uma imagem “cópia”, cópia esta que será utilizada para comparar a semelhança entre a imagem de entrada e a imagem redimensionada.

Na terceira fase - formação de modelos- “o hacker pode adulterar o conjunto de treino para manipular o comportamento de inferência do modelo.” (Hu et al., 2021, p.9) O ataque que cumpre a adulteração do modelo de treino do sistema pode ser de duas naturezas: ataque à disponibilidade e ataque à integridade. Segundo os autores (Hu et al., 2021) no ataque à disponibilidade, o objetivo do ataque é maximizar a perda global do modelo e causar uma degradação no desempenho do modelo, por seu turno o ataque à integridade do sistema consiste na introdução calculada no modelo de treino de dados enviesados dentro do conjunto de dados fiáveis de modo a condicionar o resultado. Para solucionar esta falha é recomendável proceder à análise dos dados inseridos no modelo de treino de modo a detetar anomalias ou em alternativa é recomendável reforçar a robustez do modelo de treino.

Na quarta fase- inferências do modelo - conforme explana Hu et al. (2021) a uma amostra validada (x) a partir da qual se fazem inferências- $f(x) = y_{true}$, o hacker adiciona uma perturbação impercetível (δ) à amostra (x) para criar um exemplo contraditório $x' = x + \delta$, que é suficiente para induzir o modelo em erro e produzir um resultado errado- $f(x) \neq y_{true}$. Por outras palavras a desvirtuação do processo ocorre através da introdução calculada de uma perturbação no conjunto da amostra para induzir o modelo de inferência a interpretar erradamente. Este tipo de ataque, intitulado de ataque adversarial a sistemas de classificação, pode ser combatido através de diversas estratégias, entre as quais a alteração do sistema, o melhoramento do modelo, o acréscimo de sistema, a validação do sistema ou a alteração do método do modelo de inferência e dos dados inseridos. (Hu et al., 2021)

Na quinta fase- integração do sistema - os principais aspetos a considerar são a manutenção da confidencialidade -dados, informações sobre o sistema e seu modo de funcionamento- e a proteção do código de funcionamento do sistema informático. (Hu et al.,2021) Para solucionar possíveis ameaças à confidencialidade e proteger o código de funcionamento do sistema informático Hu et al. (2021) recomendam, no tocante ao hardware, a modificação e verificação das propriedades físicas dos sensores, no tocante ao software, recomendam a conceção de estratégias conducentes à identificação e rejeição de sinais maliciosos durante a fase de recolha de dados do sensor; mais sugerem que para melhorar a interoperabilidade dentro dos modelos de IA é necessário congregiar o tratamento das questões de confidencialidade às questões de segurança de modo a reforçar a dupla proteção dos sistemas de IA.

Também incluído na vertente das vulnerabilidades tecnológicas, mas especificamente relacionado com a gestão da segurança de dados de sistemas de videovigilância que empregam a IA, Myagmar-Ochir e Kim (2023) salientam a importância de garantir a gestão segura de dados produzidos por estes sistemas. “A segurança de dados num [CCTV] refere-se à proteção contra o acesso não autorizado, a adulteração ou a perda de imagens de vídeo e outros dados relacionados capturados.” (Myagmar-Ochir e Kim, 2023, p.21) Para garantir a legalidade dos dados produzidos, mais precisamente a produção e recolha de imagens, é “necessário limitar a gravação de vídeo a uma determinada parte do campo de visão da câmara” (Myagmar-Ochir e Kim, 2023, p.21) de modo a não captar zonas nas quais a captação de imagens não é permitida por questões de privacidade. Para garantir a autenticidade dos dados produzidos, previamente à recolha de dados, é necessário garantir “que apenas os dispositivos registados podem enviar dados para o sistema” (Myagmar-Ochir e Kim, 2023, p.21) e para garantir a originalidade (Myagmar-Ochir e Kim, 2023) dos dados recolhidos pode ser utilizada tecnologia de *blockchain* para impedir a adulteração dos ficheiros e criptografar os ficheiros.

Elucidando os conceitos acima indicados, o conceito de criptografia, conforme Magioni (2021) é o processo de codificação dos dados para que apenas elementos autorizados possam, através de uma chave, compreender a informação, trata-se de converter texto ou números legíveis por humanos num conteúdo incompreensível sem a chave de descriptação- sequência de valores matemáticos decidida pelo remetente e pelo destinatário da mensagem codificada. Relativamente ao *blockchain* (IBM, 2024), é uma

tecnologia que funciona como um livro-mestre partilhado e imutável que agrega os diferentes blocos de informação; à medida que cada evento ocorre, é registado como um “bloco” de dados, cada um dos blocos está ligado aos demais e os eventos são incluídos e bloqueados numa cadeia irreversível: uma blockchain.

6.2. ENQUADRAMENTO LEGAL CCTV EM PORTUGAL

O recurso à captação de imagens da via pública para uso das forças de segurança surgiu num contexto atípico, não foi resultado de um longo processo decisório, mas sim de adaptação às circunstâncias. Surgiu no contexto do evento desportivo que Portugal e Espanha acolheram em 2004, o campeonato europeu de futebol. Face à grande afluência de pessoas, o sistema de segurança instalado não tinha capacidade de dar resposta em tempo útil às necessidades das Forças e Serviços de Segurança, pelo que tendo em vista a eficácia foi permitido em regime temporário, pela Lei orgânica n.º 2/2004, de 12 de maio, a instalação temporária de aparelhos de vigilância eletrónica, cuja autorização vigoraria entre 1 de junho a 11 de julho de 2004.

Findo o regime excecional, o passo seguinte foi a permissão em 2005 da instalação dessa funcionalidade em regime geral, ou seja, em ambiente ordinário. A aprovação da Lei n.º 1/2005, de 10 de janeiro, marcou a oficialização da permissão em regime ordinário da videovigilância de locais públicos em Portugal. A Lei n.º 1/2005, de 10 de janeiro (2005) autorizava a utilização de videovigilância para um dos seguintes fins: a) para proteção de edifícios e instalações públicos e respetivos acessos; b) para proteção de instalações com interesse para a defesa nacional; ou, c) para proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de crimes em locais em que exista razoável risco da sua ocorrência.

Para a implementação do sistema era necessário um pedido de autorização para a instalação requerido pelo dirigente máximo da força ou serviço de segurança ou pelo presidente da câmara, esse pedido em seguida seria alvo de apreciação por parte do membro do Governo da tutela e da Comissão Nacional de Proteção de Dados (CNPD), posto que se obtivesse

concordância de ambos, o órgão requerente teria autorização de utilização por um período de duração máxima de um ano.

Subsequentemente o regime foi alterado pela Lei n.º 9/2012, de 23 de fevereiro, que introduziu várias alterações. Procedeu ao alargamento das finalidades de utilização de videovigilância para abranger a prevenção de atos terroristas ou para a proteção florestal e deteção de incêndios florestais, procede ao alargamento do prazo máximo de autorização para dois anos e removeu a natureza vinculativa do parecer prévio da CNPD.

As Portarias 373/2012 e 372/2012 de 16 de novembro definem os requisitos técnicos mínimos do sistema: as câmaras de videovigilância devem ser policromáticas, permitir a iluminação, ampliação e abertura de foco que permita a deteção e reconhecimento de vultos humanos, de indivíduos ou matrículas de veículos, consoante o palco de gravação. É também ditado pela lei que deve haver sinais informativos da entrada e saída de zonas objeto de vigilância com recurso a câmaras.

Relativamente às Forças e Serviços de Segurança, atualmente a Lei n.º 95/2021, de 29 de dezembro regula a utilização e o acesso a sistemas CCTV pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC). No caso da ANEPC, cabe ao seu dirigente máximo adereçar pedidos de autorização para instalação de sistemas de videovigilância.

A Lei de Segurança Privada- Lei 34/2013, de 16 de maio- estabelece os requisitos a respeitar na instalação e exploração de um sistema de videovigilância para organismos privados. Contudo não sendo a videovigilância um recurso exclusivamente utilizado na segurança privada, é necessário a delimitação dos pressupostos a respeitar na instalação e exploração de um sistema de videovigilância por parte de organismos públicos. Para esse efeito, o Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, materializado na ordem jurídica interna na Lei n.º 58/2019, de 8 de agosto delimita “as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.” (Regulamento Geral de Proteção de Dados, 2016)

Em matéria de defesa do direito à privacidade, a CRP no disposto do art.º 26º refere-se a outros direitos pessoais, enunciando que a todos é reconhecido o direito à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à

proteção legal contra quaisquer formas de discriminação. (Constituição da República Portuguesa,1976)

A CRP elenca os direitos à imagem e à intimidade da vida privada, contudo não define a sua natureza; o Código Civil (CC) elabora o conteúdo abrangido por estes direitos. O CC explana o conteúdo do direito à imagem indicando que “o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela” (Código Civil, 1966), indica também que o direito à reserva sobre a intimidade da vida privada enquadra a guarda da intimidade da vida privada de outrem e que os limites que cerceiam esse direito variam conforme a natureza do caso e a condição das pessoas.

A videovigilância resulta na recolha de imagens por meio eletrónico que podem incluir dados pessoais, definidos pelo Regulamento Geral de Proteção de Dados como “informação relativa a uma pessoa singular identificada ou identificável.” (Regulamento Geral de Proteção de Dados, 2016) Por esse motivo, as imagens recolhidas por sistema de videovigilância, que podem incluir pessoas e objetos pessoais, estão suscetíveis à captação de dados pessoais. “Assim, a videovigilância, ao recolher imagens de pessoas, é suscetível de derrogar o direito à imagem e à reserva da vida privada.” (Alves, 2019, p. 140)

Ao nível comunitário, a União Europeia, ao abrigo do artigo 16º, nº 2 do Tratado sobre o Funcionamento da União Europeia, emitiu um regulamento que se materializou no Regulamento Geral sobre a Proteção de Dados (RGPD). Este regulamento tem a finalidade de defender “os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.” (Jornal Oficial das Comunidades Europeias, 2016)

Para fiscalizar o cumprimento dos pressupostos enunciados pelo RGPD, tornou-se necessária a criação de um organismo específico. O RGPD é aplicável às atividades que envolvam a recolha e tratamento de dados nas quais seja aplicado o direito da União Europeia. Nos termos do artigo 4º da Lei n.º 58/2019, de 8 de agosto, a Comissão Nacional de Proteção de Dados (CNPd) é uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, cuja função compreende o controlo e a fiscalização do cumprimento do RGPD, bem como das demais disposições legais e regulamentares em

matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.

Contudo como o próprio diploma elucida, as disposições contidas no Regulamento Geral sobre a Proteção de Dados não são aplicáveis às atividades desenvolvidas no âmbito da política externa e de segurança comum, às atividades privadas e particulares nem às atividades efetuadas pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Não estando a recolha e tratamento de dados no âmbito de atividades efetuadas pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública incluídas no âmbito do Regulamento Geral de Proteção de Dados, está em contrapartida submetido a um enquadramento legislativo específico. Nomeadamente sob a égide da Lei n.º 95/2021, de 29 de dezembro que regula a utilização e o acesso de sistemas CCTV por parte de instituições públicas destinadas à salvaguarda da segurança pública e no tocante ao tratamento de dados pessoais subordinado ao cumprimento dos requisitos impostos pela Lei n.º 59/2019, de 08 de agosto, que materializa na ordem interna a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

A Lei n.º 95/2021, de 29 de dezembro adota o princípio da publicidade como elemento norteador da instalação de CCTV, ordenando que nos locais que sejam objeto de vigilância com recurso a câmaras fixas e portáteis é obrigatória a afixação, em local bem visível, de informação concernente à existência e a localização das câmaras de vídeo, à finalidade da captação de imagens e sons e indicação da entidade responsável pelo tratamento dos dados recolhidos. Tendo em conta a defesa dos direitos pessoais, está vedada a captação de imagens e sons que firam “de forma direta e imediata, a esfera da reserva da vida íntima e privada” (Lei n.º 95/2021, 2021) e determina que as gravações obtidas são conservadas por um período máximo de 30 dias desde a respetiva captação.

6.3. ENQUADRAMENTO LEGAL IA EM PORTUGAL E NA UNIÃO

Respeitante à Inteligência Artificial embora floresçam planos e estratégias, juridicamente o conteúdo enunciado é esparso. No contexto português, o Decreto-Lei n. °65/2021 regulamenta o Regime Jurídico da Segurança do Ciberespaço, determinando os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais. Não incide especialmente na temática da IA, contudo contribui para a uniformização dos critérios de modo a assegurar o seguro uso do espaço tecnológico. Outro documento importante no contexto nacional é a Carta Portuguesa de Direitos Humanos na Era Digital. Este documento estabelece os princípios que devem reger o uso da inteligência artificial e de robôs, nomeadamente no seu artigo 9º, indicando que “a utilização da inteligência artificial deve ser orientada pelo respeito dos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência e da responsabilidade.” (Lei n.º 27/2021, 2021)

No contexto comunitário, a Carta Europeia de ética sobre o uso da inteligência artificial em sistemas judiciais e seu ambiente, adotada pela Comissão Europeia para a Eficácia da Justiça em 2018, enuncia os cinco princípios de devem nortear o uso de aplicações de IA no processos e decisões judiciais, nomeadamente o princípio do respeito dos direitos fundamentais, o princípio da não discriminação, o princípio da qualidade e da segurança, o princípio da transparência e o princípio do controlo dos utilizadores.

A Declaração Europeia sobre os direitos e princípios digitais para a década digital (2022), focando-se no pleno respeito dos direitos fundamentais das pessoas e na proteção contra os riscos e os danos associados ao uso da inteligência artificial, avança a necessidade de assegurar a transparência sobre a utilização de algoritmos e inteligência artificial, bem como impedir que essas ferramentas sejam utilizadas para determinar previamente as escolhas das pessoas.

O Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial está previsto entrar em vigor no dia 1 de agosto de 2024. Constitui um esforço legislativo da União Europeia que vem sendo debatido nos últimos três anos. Sendo a matéria legislada em forma de

Regulamento, a sua aplicação é geral e não carece de qualquer transposição pelos Estados-membros pelo que entra em vigor em todos os Estados na data fixada. O referido regulamento tendo “por objetivo a melhoria do funcionamento do mercado interno mediante a previsão de um regime jurídico uniforme” (Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024), procura fomentar “o desenvolvimento, a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial.” (Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, 2024)

Esta iniciativa constitui um marco a nível internacional, cujo objetivo geral pode ser decomposto em quatro linhas principais (Sousa, 2023): assegurar que os sistemas de IA respeitam os valores éticos da UE e a legislação em vigor sobre direitos fundamentais, garantir a segurança jurídica de forma a atrair investimento na área tecnológica, promover uma boa governação que permita uma IA conforme aos direitos fundamentais e promover um mercado único e uniforme para os sistemas e aplicações de IA.

No âmbito do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (2024), o uso por parte das forças e serviços de segurança em espaço público de IA para a deteção precoce de atividades que ameacem a ordem pública determina que este tipo de sistema seja enquadrado como Sistemas de IA de risco elevado. Pois, nos termos do anexo dois do Regulamento que cria regras harmonizadas em matéria de inteligência artificial, sistema de risco elevado incluem:

Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular cometer uma infração penal não exclusivamente com base na definição de perfis de pessoas singulares. (Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, 2024)

7. ESTUDO DE CASO

Em Portugal, os municípios de Leiria e de Portimão foram pioneiros no tocante à utilização de IA em sistemas de CCTV para a repressão da criminalidade. (Nabais, 2023) Ambos os municípios, o município de Leiria pretendendo a adição ao sistema de videovigilância instalado funcionalidades de IA e o município de Portimão pretendendo a instalação de um sistema de videovigilância com funcionalidades de IA, pretendiam fazer uso da tecnologia disponível para combater ameaças à segurança pública. Em ambos os casos, a CNPD, na sua qualidade de órgão consultivo que emite pareceres não vinculativos, emitiu pareceres negativos realçando o impacto negativo que a instalação de sistemas CCTV teria na privacidade dos cidadãos e frisando o impacto negativo que a utilização de tecnologia de *soft recognition* (termo utilizado pelo redator do relatório) tem para a privacidades das pessoas, nomeadamente atentando contra a liberdade e o direito à igualdade.

A CNPD, no seu Parecer 209/92, considera

Evidente que a utilização de IA, em especial quando utilizada num ambiente de controlo sistemático e em larga escala de zonas acessíveis ao público, tem de ser precedida de uma cuidadosa ponderação das consequências da mesma, não apenas para a privacidade das pessoas, como também a liberdade, a identidade pessoal e o direito à não discriminação. (Comissão Nacional de Proteção de Dados, 2019)

No tocante à opinião dos cidadãos que navegam os locais incluídos em zonas monitoradas por sistemas de CCTV, Cardoso conduziu em 2023 um estudo, como o próprio frisa, “da população em geral, ainda que de forma estatisticamente não representativa” (Cardoso, 2022, p. 20) devido ao facto de compreender 160 respostas unicamente fornecidas por internautas. Por forma a avaliar diversas questões, indagou se a idade ou a escolaridade afetariam a opinião do indivíduo sobre a videovigilância do espaço público, se a opinião do indivíduo varia consoante a experiência pessoal com as câmaras de videovigilância, se a concordância com instalação de mais câmaras está relacionada com a opinião do indivíduo sobre a videovigilância, se a satisfação do indivíduo no que toca à videovigilância atual da

sua freguesia de residência influencia a sua vontade de instalação de mais câmaras e por último se a videovigilância do espaço público condiciona os seus comportamentos.

No que diz respeito à influência da idade e da escolaridade na opinião do indivíduo sobre a videovigilância do espaço público, não foram encontradas evidências que sugiram que estas influenciam a opinião sobre a videovigilância. Em relação à influência da experiência pessoal com as câmaras de videovigilância, verificou-se que “a existência de experiências pessoais em que a presença de câmaras de videovigilância foi relevante condiciona a opinião dos participantes no que respeita à videovigilância do espaço público.” (Cardoso, 2022, p. 50) Tendo em consideração a concordância com instalação de mais câmaras, foi demonstrado que esta variável está relacionada com a opinião pessoal sobre a videovigilância. É de salientar que a satisfação do indivíduo no que toca à videovigilância atual da sua freguesia de residência não influencia a sua vontade para a instalação de mais câmaras.

Concernente à relação entre a alteração dos seus comportamentos e a opinião dos inquiridos sobre a videovigilância do espaço público, constatou-se que 94% dos inquiridos não alterou o seu comportamento depois da instalação de câmaras de videovigilância por oposição a 4% de inquiridos que alteraram o seu comportamento depois da instalação de câmaras de videovigilância. (Cardoso, 2022)

Avançando para um contexto mais tangível, o Bairro Alto merece destaque entre os locais em Portugal onde existem sistemas CCTV por representar o primeiro local onde foi instalado este tipo de sistema. O sistema videovigilância instalado no Bairro Alto foi aprovado em 2009, pelo Despacho 27484/2009, de 23 de dezembro, só tendo entrado em funcionamento alguns anos mais tarde, nomeadamente em 2014.

O Bairro Alto localiza-se na cidade de Lisboa, pertencendo à freguesia da Misericórdia. Esta freguesia compreende uma área de 1,1 km² da área total da cidade de Lisboa, detendo 207 arruamentos no total da sua área. Destes 207 arruamentos, 41 fazem parte do Bairro Alto. Possuindo uma arquitetura distinta, o aglomerado populacional é delimitado a norte, pela rua D. Pedro V, a sul pela calçada do Combro, largo do Calhariz e rua do Loreto, a este pela rua da Misericórdia e rua de São Pedro de Alcântara e a oeste pela rua do Século.

Segundo os dados apurados pelos Censos de 2021, a freguesia da Misericórdia apresenta uma densidade populacional de 4.410 habitantes por quilómetro quadrado, bastante

envelhecida, apresentando um índice de envelhecimento de 234 idosos por cada 100 jovens. Apesar da afluência diária no território desta freguesia em particular, em termos absolutos perdeu população residente, pois tendo em conta os dados obtidos nos Censos de 2011, sofreu uma perda populacional na ordem dos 26% face a 2001.

Na freguesia da Misericórdia, nas palavras de Regino (2023) apresenta uma grande densidade populacional, que se verifica em determinadas horas do dia e da noite, o facto derivado de a localidade compreender não só áreas de comércio e de diversão noturna bastante movimentadas e conhecida durante todo o ano como também diversos locais de culto. Aglomerado de contrastes “da grande afluência de cidadãos de camadas jovens no período noturno, [e a] confusão e diversão noturna que daí resulta, passamos para um ambiente diurno pacato, silencioso e quase intimista” (Pires, 2016, p. 40), o arruamento estreito fomenta tanto o sentimento de privacidade como a ocorrência de condutas desordeiras.

Analisando os dados fornecidos pelo Turismo de Portugal (2024), pertencente ao Ministério da Economia e do Mar, no ano de 2023, na Área Metropolitana de Lisboa, registaram-se um total superior a 8 milhões de hóspedes, sendo a maioria destes estrangeiros. Tendo em consideração o impacto do turismo no Produto Interno Bruto, contribuindo em 9,5% para a riqueza nacional, que em termos absolutos representa 25 mil milhões de euros, não será despendendo fomentar a promoção de condições de segurança para atrair e manter o turismo.

Em linha com as conclusões apresentadas no RASI de 2023, a criminalidade em geral aumentou também no município de Lisboa. Os dados mais recentes disponibilizados pelo Pordata (2024) indicam que os crimes contra pessoas aumentaram.

No ano de 2022 foram reportadas 5413 incidências quando no ano de 2023 se situavam já em 5602 incidências. O aumento em termos absolutos pode à primeira vista não merecer escrutínio pois traduz-se num aumento de 3,0% face ao período homólogo anterior, contudo o aumento paulatino, mas constante da criminalidade contra pessoas verifica-se constante nos últimos três anos, tendo já atingido valores superiores aos registados em 2018. Também os crimes contra o património registaram um aumento em relação ao ano de 2022; quando em 2022 se registaram 18631 crimes contra o património em Lisboa, no ano seguinte -2023- essa contabilização elevou-se a 20424 ocorrências. Um aumento de 9% face ao período homólogo anterior.

Os crimes previstos em legislação avulsa revelaram um decréscimo face ao ano de 2022. No ano de 2023 foram registados em Lisboa 4290 eventos, enquanto no ano anterior tinham sido registadas 4339, uma diminuição de 1%, estatisticamente pouco relevante, mas importante em termos do custo humano associado à prática de qualquer ato criminoso. Em contrapartida, os crimes contra a vida em sociedade, onde estão incluídas a título de exemplo a criminalidade derivada de participação em motim ou da associação criminosa, revelaram um comportamento estatístico inverso à tendência geral. No município de Lisboa nos últimos 2 anos ocorreu uma diminuição da criminalidade contra a vida em sociedade, tendo o ano de 2023 somado 2597 ocorrências e o ano de 2022 as 3246 ocorrências, tendo-se registado uma impressionante redução em 20% face ao período homólogo anterior.

Face aos dados estatísticos inquietantes, tendo já a instalação de CCTV no Bairro Alto contribuído para a redução da criminalidade e do sentimento de insegurança (Pires, 2016), seria talvez oportuno melhorar a capacidade do sistema de CCTV instalado por forma a utilizar IA na prevenção da criminalidade em geral, com especial foco na prevenção de incivildades e de criminalidade violenta.

8. CONCLUSÃO

A única constante da vida é a mudança, todo o organismo, seja ele animado ou inanimado, está em constante evolução. Essa mudança pode ser mais visível ou menos visível, pode ser mais veloz ou menos veloz, mas nada é eterno. Tal como evolui a sofisticação do génio humano também o crime, fenómeno inerentemente humano, acompanha a evolução na sofisticação. As organizações do crime e os indivíduos que o praticam recorrem de todos os meios disponíveis para atingir os seus objetivos, a utilização de meios tecnológicos também está incluída. A criminalidade evolui, portanto, as ações para o seu combate também devem evoluir.

A videovigilância aliada à ação do agente da lei surge como meio preferencial para o combate de fenómenos criminógenos pois esta permite racionalizar os recursos, diminuir o risco para os primeiros intervenientes e graças à informação visual recolhida, aumentar a eficácia da resposta a situações de necessidade bem como aumentar as hipóteses de detenção em virtude da maior visibilidade dos infratores.

As imagens captadas pelos sistemas CCTV não têm a função, num Estado de Direito Democrático, de controlar todos os aspetos da vida do cidadão, mas sim evidenciar e adereçar comportamentos desviantes e criminosos.

A cidade inteligente deve fazer uso dos meios tecnológicos ao seu dispor de forma a melhor gerir os seus recursos e dessa forma melhorar a qualidade de vida dos seus cidadãos e minimizar o desperdício de recursos.

A introdução de ferramentas de Inteligência Artificial visa através da deteção de anomalias comportamentais- incivilidades e atos criminosos- precocemente aumentar a produtividade do visionamento e minimizar o tempo de resposta. Esses benefícios podem ser alcançados através de softwares cuja capacidade de análise e predição permite processar grandes quantidades de dados e executar tarefas complexas, ultrapassando a normal cognição humana.

9. BIBLIOGRAFIA

Agra, C., Guedes, I., Cardoso, C. (2012). Medo do crime: Revisão conceptual e metodológica. In Agra, A.- *A Criminologia: Um arquipélago interdisciplinar*. 1ªed. Porto: Universidade do Porto. 2012. Cap 8, p. 213-249

Aguiar, J. (1989). *A Política de Defesa Nacional como Política Pública interdepartamental*. Instituto de Defesa Nacional. Lisboa. Instituto Nacional De Administração.

Alves, L. (2019). A videovigilância e a compressão da privacidade. *Anuário da Proteção de Dados*. p. 137–155. <https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/6.-Lurdes-Dias-Alves.pdf>

Anderez, D. et al. (2021). The Rise of Technology in Crime Prevention: Opportunities, Challenges and Practitioners Perspectives. *arXiv*, 2102.04204. <http://arxiv.org/abs/2102.04204>

Bauman, Z. (1989). *A Liberdade*. Lisboa. Editorial Estampa.

Bentham, J. (1995). Panopticon; Or, The Inspection-House: Containing The Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in which Persons of Any Description are to be Kept Under Inspection: And In Particular To Penitentiary-Houses, Prisons, Houses Of Industry, Work-Houses, Poor Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals, And Schools: With A Plan Of Management . In Bozovic, M., *The Panopticon Writings*. p. 29-95 https://ics.uci.edu/~djp3/classes/2012_01_INF241/papers/PANOPTICON.pdf

Brantingham, P., Brantingham, P. (1981). *Environmental criminology*. Beverly Hills. Sage Publications.

Brantingham, P., Faust, F. (1976). A Conceptual Model of Crime Prevention. *Crime & Delinquency*, 22(3), p. 284–296. <https://doi.org/10.1177/001112877602200302>

Cai, K., Wang, J. (2009). Urban design based on public safety—Discussion on safety-based urban design. *Frontiers of Architecture and Civil Engineering in China*, 3(2), p. 219–227. <https://doi.org/10.1007/s11709-009-0023-4>

Câmara Municipal da Amadora. (2022). *Sistema de Videoproteção*. <https://www.cm-amadora.pt/pt/6654-sistema-de-videoprotecao.html> Acedido em 28 de junho de 2024.

Camões, L. (1971). *Poesia Lírica*. Biblioteca Básica Verbo.

Cardim, M. (2007). Implementação de Políticas Públicas – Do Discurso às Práticas. *Cadernos Sociedade e Trabalho*, 10, p.141-160

Cardoso, G. (2022). The big brother experience: Oportunidades e ameaças de um sistema de videovigilância no concelho da Amadora. Lisboa: Instituto Universitário de Lisboa. Dissertação de mestrado. <https://repositorio.iscte-iul.pt/handle/10071/27704> Acedido em 31 de janeiro de 2024.

Carvalho, I. (2020). Sistema de videovigilância na freguesia de Águas Livres: Efeitos na criminalidade. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Dissertação de mestrado. https://comum.rcaap.pt/bitstream/10400.26/32978/1/155861_Carvalho_Sistema-de-videovigil%C3%A2ncia-na-freguesia-de-%C3%81guas-Livres-Efeitos-na-criminalidade_VERSAOFINAL.pdf Acedido em 07 de março de 2024.

Castillo, J. (2011). Sistemas de videovigilancia y CCTV. <http://myelectronic.byethost10.com/Mis%20proyectos/Sistemas%20de%20videovigilancia%20y%20CCTV.PDF?i=1>

Caupers, J. (2007). *Introdução ao Direito Administrativo*. (9ªed.) Âncora.

Chartrand, G. et al. (2017). Deep Learning: A Primer for Radiologists. *RadioGraphics*, 37(7), p.2113–2131. <https://doi.org/10.1148/rg.2017170077>

Chen, C., Surette, R., & Shah, M. (2021). Automated monitoring for security camera networks: Promise from computer vision labs. *Security Journal*, 34(3), p. 389–409. <https://doi.org/10.1057/s41284-020-00230-w>

Clarke, R., Cornish, D. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice: A Review of Research*, 6, p. 147–185. http://users.soc.umn.edu/~uggen/Clarke_85.pdf

Clemente, P. (2010). Polícia e segurança: Breves notas. *Lusíada. Política internacional e segurança*, 4, p. 139-169. <https://doi.org/10.34628/PFQ5-KZ27>

Clemente, P. (2013). Prevenção e Segurança: Política e estratégia. In Almeida, P. Como tornar Portugal seguro? Segurança Nacional e Prevenção da Criminalidade. Lisboa. Bnomics. p. 35-57

Clemente, P. (2016). *Ética Policial- da eticidade da coação policial*. Instituto Superior de Ciências Policiais e Segurança Interna.

Cohen, L. Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), p.588–608.

Cusson, M. (2011). *Criminologia*. (3ªed.) Casa das Letras.

Damon, J. (2000). Les «incivilités». *Revue des politiques sociales et familiales*. 60, p. 139–142.

Direção-Geral da Política de Justiça. (2024) *Sistema de Justiça Português*. <https://dgpj.justica.gov.pt/Dossiers-tematicos/Sistema-de-Justica-Portugues>
Acedido em 17 de junho de 2024.

Dijk, J., & Waard, J. (1991). A two-dimensional typology of crime prevention projects: With a bibliography. *Criminal justice abstracts*, p. 483–503.

Durkheim, E. (1991). *As regras do método sociológico*. (4ªed.) Editorial Presença.

Dye, T. (1975). *Understanding Public Policy* (8ª ed.) Englewood cliffs.

Eckblom, P. (1996, setembro, 43-98). *Towards a Discipline of Crime Prevention: A Systematic Approach to its Nature, Range and Concepts*. 22ª Conferência Preventing Crime and Disorder, Londres.

Ferreira, E. (2003). Violência e Insegurança Urbana: Um Fenómeno em Crescimento ou em Transformação? O Caso da Área Metropolitana de Lisboa. *CIDADES, Comunidades e Territórios*, 7, p.37-57 <https://revistas.rcaap.pt/cct/article/view/9176>

Figueiredo, A., Guilhem, D. (2008). Ética e Moral. *Revista Internacional Interdisciplinar*, 5, p. 29–46.
<https://www.researchgate.net/publication/38101200> *Etica Moral Ethics and Moral*

Fonseca, F. (2010). A evolução das políticas públicas de segurança interna em Portugal, na era da globalização. Lisboa: Universidade Técnica de Lisboa.
Dissertação de

mestrado. https://www.repository.utl.pt/bitstream/10400.5/2977/1/Tese_Francisco%20Jos%C3%A9%20Seixas%20Fonseca.pdf Acedido em 6 de julho de 2024.

Foucault, M. (2001). *Vigiar e Punir*. (24ªed.) Vozes

Fróis, C. (2011). *Vigilância e Poder*. Mundos Sociais.

Goffman, E. (1963). Behavior in Public Places [em linha]. Nova Iorque: The free pres. [28 maio 2024] Disponível em: <https://osf.io/zth8x>

Goldstein, H. (1979). Improving Policing: A Problem-Oriented Approach. *Crime & Delinquency*, 25(2), p. 236–258. <https://doi.org/10.1177/001112877902500207>

Goold, B. (2004). *CCTV and Policing Public Area Surveillance and Police Practices in Britain*. Oxford University Press.

Haenlein, M., Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61(4), p.5–14. <https://doi.org/10.1177/0008125619864925>

Heimbach, D. (2015). How the Term «Ethics» Has Evolved. Ethics & Religious Liberty Commission <https://erlc.com/resource-library/articles/how-the-term-ethics-has-evolved/> Acedido em 3 de maio de 2024.

Henry, S., Howard, L. (2018). *Social Deviance* (2ª ed.). John Wiley & Sons.

Hobbes, T. (2005). *Of Man. The life of man, solitary, poore, nasty, brutish and short*. Penguin Books

Hu, Y., et al. (2021). Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys*, 55(1), p.1-36. <https://doi.org/10.1145/3487890>

Hunter, A. (1978, novembro, 8-12). *Symbols of Incivility: Social Disorder and Fear of Crime in Urban Neighborhoods*. Annual meeting of the american criminological society, Dallas.

IBM. (2021a, março 15). *Supervised vs Unsupervised Learning*. <https://www.ibm.com/think/topics/supervised-vs-unsupervised-learning> Acedido em 2 de julho de 2024.

IBM. (2021b, julho 27). *What is Computer Vision?* IBM. <https://www.ibm.com/topics/computer-vision> Acedido em 23 de julho de 2024.

IBM. (2024). What Is Blockchain? <https://www.ibm.com/topics/blockchain> Acedido em 26 de julho de 2024.

Instituto Nacional de Estatística. (2021). *Censos 2021*. <https://app.powerbi.com/view?r=eyJrIjoiMTIjM2IwMzMtN2E4Zi00NjY2LTkxOTQtMDA4NTZjZTJhNTkzIiwidCI6IjcxOTQwYTg2LTUyYmQtNGVhMy04OWI3LWUwYTdjZDcwNDA0MyIsImMiOiJ9> Acedido em 26 de julho de 2024.

Instituto Nacional de Estatística. (2022). *Crimes registados pelas autoridades policiais por Localização geográfica e Categoria de crime; Anual*. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0008073&contexto=bd&selTab=tab2 Acedido em 26 de julho de 2024.

Idrees, H., Shah, M., & Surette, R. (2018). Enhancing camera surveillance using computer vision: A research note. *Policing: An International Journal*, 41(2), p. 292–307. <https://doi.org/10.1108/PIJPSM-11-2016-0158>

Institute for Economics & Peace. (2023). *Global Peace Index 2023: Measuring Peace in a Complex World*. <https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf> Acedido em 15 de julho de 2024.

Jakhar, D., & Kaur, I. (2020). Artificial intelligence, machine learning and deep learning: Definitions and differences. *Clinical and Experimental Dermatology*, 45(1), p.131–132. <https://doi.org/10.1111/ced.14029>

Kant, I. (1996). *Fundamentação da Metafísica dos Costumes*. Edições 70.

Kant, I. (1992). *A Paz Perpétua e outros opúsculos*. Edições 70.

Kim, B., et al. (2020). Decamouflage: A Framework to Detect Image-Scaling Attacks on Convolutional Neural Networks. *ArXiv: abs/2010.03735*. <https://www.semanticscholar.org/paper/deee7568259fb7bf58949440c9c137d808fbb865>

Laufs, J. (2022). *Crime Prevention and Detection Technologies in Smart Cities: Opportunities and Challenges*. Londres: University College London. Dissertação de doutoramento.

https://discovery.ucl.ac.uk/id/eprint/10147500/1/PhD%20Thesis_compressed.pdf
Acedido em 07 de março de 2024.

- Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, 55. <https://doi.org/10.1016/j.scs.2020.102023>
- Maggioni, M. (2021). Smart Cities, Eco-Cities, and urban security. Roma: Libera Università Internazionale degli Studi Sociali Guido Carli. Dissertação de mestrado. https://tesi.luiss.it/30380/1/641712_MAGGIONI_MARTINA.pdf
- Maguire, M., Morgan, R., & Reiner, R. (Eds.). (1997). *The Oxford handbook of criminology* (2^o ed.). Oxford University Press.
- Martins, F. (S/N). *O advogado em casa*. Editorial Verbo.
- Milburn, P. (2000). Violence et incivilités: De la rhétorique experte à la réalité ordinaire des illégalismes. *Déviance et société*, 24(4), p. 331–350. <https://doi.org/10.3406/ds.2000.1735>
- Monteiro, J. (2000). Caracterização dos Espaços Urbanos na RLVT: O contributo da análise discriminante. *Estudos Regionais*, 2^o semestre.
- Morgado, S., & Felgueiras, S. (2022). Technological Policing: Big data vs real data. *Politeia*, XIX, p.139-151. <https://doi.org/10.57776/0PEP-XZ31>
- Munakata, T. (Ed.). (2007). *Fundamentals of the New Artificial Intelligence*. Springer London. <http://link.springer.com/10.1007/978-1-84628-839-5>
- Myagmar-Ochir, Y., Kim, W. (2023). A Survey of Video Surveillance Systems in Smart City. *Electronics*, 12(17). <https://doi.org/10.3390/electronics12173567>
- Nabais, T. (2023). Proteção de Espaços Públicos: Sistemas de Videovigilância Inteligentes. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Trabalho de Investigação final. https://comum.rcaap.pt/bitstream/10400.26/45992/1/F05%20-%20TIF-Tiago%20Nabais-Protec%cc%a7a%cc%83o%20de%20espac%cc%a7os%20pu%cc%81blicos_Sistemas%20de%20videovigila%cc%82ncia%20inteligentes-152484.pdf Acedido em 31 de janeiro de 2024.

- Nadikattu, R. (2019). New Ways in Artificial Intelligence. *International journal of computer trends and technology*, 67(12), p. 89-94. <https://doi.org/10.2139/ssrn.3629063>
- Norris, C., & Wilson, D. (2017). Surveillance, Crime and Social Control. *Crime Prevention Studies*, 10, p. 157–178. [https://www.researchgate.net/publication/240622230 CCTV and the social structuring of surveillance](https://www.researchgate.net/publication/240622230_CCTV_and_the_social_structuring_of_surveillance)
- Paludo, A. V. (2010). *Administração Pública Teoria e mais 500 questões*. Elsevier.
- Paludo, A. V. (2021). *Questões Comentadas de Administração Pública [em linha] (4ªed.)*. Curitiba:Editora Jus Podivm. [6 junho 2024] Disponível em: https://juspodivmdigital.com.br/cdn/arquivos/jus1914_atualizacao.pdf
- Pateman, T. (2011). Rural and urban areas: Comparing lives using rural/urban classifications. *Regional Trends*, 43(1), p. 11–86. <https://doi.org/10.1057/rt.2011.2>
- Pereira, P. (2017). *Políticas de segurança e a videovigilância urbana—O caso da Amadora*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Trabalho de Investigação Final <https://comum.rcaap.pt/handle/10400.26/35180> Acedido em 8 de dezembro de 2023.
- Pereira, N. (2020). *O Impacto das Câmaras de Videovigilância no Sentimento de Insegurança: Um Estudo Experimental*. Porto: Faculdade de Direito da Universidade do Porto. Dissertação de Mestrado. <https://repositorio-aberto.up.pt/bitstream/10216/131658/2/437736.pdf> Acedido em 9 de abril de 2024.
- Pires, P. (2016). *Dos efeitos dos sistemas de videovigilância (CCTV) na criminalidade e sentimento de insegurança da população*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Dissertação de Mestrado <https://comum.rcaap.pt/handle/10400.26/15542?locale=en> Acedido em 31 de janeiro de 2024.
- Piza, E. et al. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), p.135–159. <https://doi.org/10.1111/1745-9133.12419>

Pordata. (2023). *Temas em construção*. <https://www.pordata.pt/pt/documentos-indicadores> Acedido em 2 de agosto de 2024.

Portal do Ministério Público- Portugal. (2024) Jurisdição Penal <https://www.ministeriopublico.pt/pagina/jurisdicao-penal> Acedido em 17 de junho de 2024.

Quaresma, C. (2021). A medição do crime e o caso particular da criminalidade violenta em Portugal. *Politeia*, XVIII, p. 83–114. <https://politeia-online.pt/wp-content/uploads/2021/09/Carina-Quaresma.pdf>

Ramaprasad, A., Sanchez, A., Syn, T. (2017, agosto). *Ontological Review of Smart City Research*. Twentythird Americas Conference on Information Systems, Boston. <https://aisel.aisnet.org/amcis2017/eGovernment/Presentations/4/>

Ramaprasad, A., Sánchez-Ortiz, A., Syn, T. (2017, agosto p.13–24). *A Unified Definition of a Smart City*. Electronic Government Springer International Publishing, São Petersburgo, https://doi.org/10.1007/978-3-319-64677-0_2

Ratcliffe, J. Rosenthal, J. (2021). *Video surveillance of public places*. U.S. Department of Justice. Problem-Oriented Guides for Police https://popcenter.asu.edu/sites/default/files/video_surveillance_of_public_places_2_d_ed_9.1.22.pdf

Ratcliffe, J., Taniguchi, T., Taylor, R. (2009). *The Crime Reduction Effects of Public CCTV Cameras: A Multi-Method Spatial Approach*. *Justice*, 26, p.746-770 <https://doi.org/10.1080/07418820902873852>

Reckless, W. (1940). *Criminal Behavior*. [Em linha] Iorque: Mcgraw-hill Book Company, Inc. [15 maio 2024] Disponível em: <http://archive.org/details/dli.ernet.166235>

Regino, J. (2023). *Proteção de Soft Targets: A Ameaça de terrorismo na Área do Bairro Alto*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Dissertação de Mestrado. https://comum.rcaap.pt/bitstream/10400.26/45744/1/Disserta%c3%a7%c3%a3o_Mestrado_157278_JoaoRegino.pdf Acedido em 31 de janeiro de 2024.

Roché, S. (2002). *Tolérance zéro Incivilités et insecurity*. Odile Jacob.

Rousseau, J. (1761). A discourse upon the origin and foundation of the inequality among mankind. [Em linha] Londres, R. and J. Dodsley. [8 junho 2024] Disponível em: <http://archive.org/details/discourseuponor00rous>

Saraiva, M. et al. (2019). A Prevenção Criminal Através do Espaço Construído (CPTED) Em Portugal: Revisão da Literatura e Redes de Conhecimento. *Revista Portuguesa de Estudos Regionais*, p. 71–93. <https://doi.org/10.59072/rper.vi52.465>

Scott, A., Gilbert, A., Gelan, A. (2007). The Urban-Rural Divide: Myth or Reality? *Macaulay Institute*.
https://www.researchgate.net/publication/253027426_The_Urban-Rural_Divide_Myth_or_Reality

Secretaria-Geral do Ministério da Justiça. (2024) *Justiça criminal*.
<https://justica.gov.pt/Justica-criminal> Acedido em 17 de junho de 2024.

Shubhendu, S., Vijay, J. (2013). Applicability of Artificial Intelligence in Different Fields of Life. *International Journal of Scientific Engineering and Research*, 1(1), p.28–35. <https://www.semanticscholar.org/paper/Applicability-of-Artificial-Intelligence-in-Fields-Shubhendu-Vijay/2480a71ef5e5a2b1f4a9217a0432c0c974c6c28c>

Sistema de Segurança Interna. (2023). *Relatório Anual de Segurança Interna*.
<https://ssi.gov.pt/comunicacao/noticias/rasi-2023/RASI%202023.pdf> Acedido em 7 de julho de 2024.

Sousa, A. (2023). *Manual de Direito Policial*. Vida Económica

Sousa, J. (2009). Videovigilância e prevenção da criminalidade. Lisboa: Academia Militar. Trabalho de investigação aplicada
<https://comum.rcaap.pt/handle/10400.26/8086> Acedido em 31 de janeiro de 2024.

Sousa, S. (2023). Breves notas sobre a “Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União.” In Sousa, S. (Coord), *A Proposta de Regulamento Europeu sobre Inteligência Artificial algumas questões jurídicas* (p. 1–15). Instituto Jurídico Faculdade de Direito da Universidade de Coimbra.
https://www.uc.pt/site/assets/files/1184561/a_proposta_de_regulamento_ebook.pdf

Tappan, P. (1947). Who is the Criminal? *American Sociological Review*, 12(1), p. 96-102. <https://doi.org/10.2307/2086496>

Tolan, P. (2002). Crime prevention: Focus on youth. In J.Q. Wilson, J. Petersilia (Eds.), *Crime* (p. 109-128). Oakland, CA: Institute for Contemporary Studies Press

Turing, A. (1950). Computing Machinery and Intelligence. *Mind*, 59(236), p. 433–460. <https://www.jstor.org/stable/2251299>

Wilson, J., Kelling, G. (1982). Broken Windows The police and neighborhood safety. *Atlantic Monthly*, 3(249), p. 29–38. <https://www.theatlantic.com/past/politics/crime/windows.htm>

LEGISLAÇÃO

Acórdão 16/15.2GEVCT.G1, de 21 de novembro, Tribunal da Relação de Guimarães, [Consultado 17 de junho de 2024] Disponível em <http://www.gde.mj.pt/jtrg.nsf/c3fb530030ea1c61802568d9005cd5bb/4857948f7f85db308025807d00502d64>

Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente. Comissão Europeia para a Eficácia da Justiça. [Consultado 17 de junho de 2024] Disponível em <https://rm.coe.int/carta-etica-traduzidapara-portugues-revista/168093b7e0>

Parecer/2019/92. Comissão Nacional de Proteção de Dados. [Consultado 17 de junho de 2024] Disponível em <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121726> Declaração Europeia sobre os direitos e princípios digitais para a década digital, de 23 de janeiro. Parlamento Europeu, Conselho, Comissão. [Consultado 17 de junho de 2024] Disponível em https://www.cnedu.pt/content/noticias/internacional/declaracao_digital_Europa.PD

Decreto-Lei nº65/2021, de 30 de julho, Diário da República, Presidência do Conselho de Ministros, Série I de 2021-07-30. [Consultado 30 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/decretolei/65-2021-168697988>

Decreto-Lei nº78/87, de 17 de fevereiro, Diário da República, Ministério da Justiça, Série I de 1987-02-17. [Consultado 7 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/decretolei/78-1987-662562>

Lei nº1/2005, de 10 de janeiro, Diário da República, Assembleia da República, Série I-A de 2005-01-10. [Consultado 27 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/lei/1-2005-457049>

Lei nº 27/2021, de 17 de maio, Diário da República, Assembleia da República, Série I de 2021-05-17. [Consultado 30 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/lei/27-2021-163442504>

Lei nº58/2019, de 8 de agosto, Diário da República, Assembleia da República, Série I de 2019-08-08. [Consultado 8 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>

Lei Orgânica nº2/2004, de 12 de maio, Diário da República, Assembleia da República, Série I-A de 2004-05-12. [Consultado 27 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/lei-organica/2-2004-264283>

Parecer nº9/96-B/Complementar, de 29 de janeiro, Ministério Público - Procuradoria-Geral da República in Diário da República, nº24, II série, de 29/01/1996. [Consultado 30 de julho de 2024] Disponível em <https://diariodarepublica.pt/dr/detalhe/parecer/9-2000-3566363>

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, 2024/1689, Eurolex. [Consultado 4 de abril de 2024] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, Parlamento Europeu, Conselho. [Consultado 28 de julho de 2024] Disponível em <https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679>

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE)

2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). [Consultado 30 de julho de 2024,] Disponível em <http://data.europa.eu/eli/reg/2024/1689/oj/por>