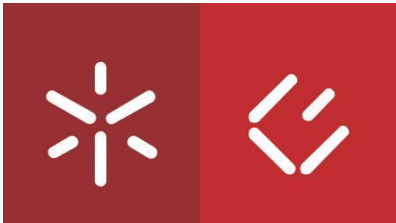


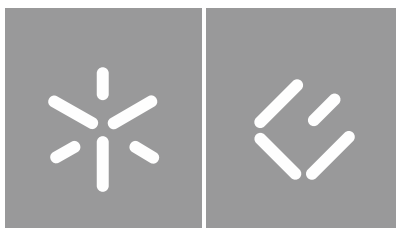


Patrícia Alexandra Gonçalves Névoa

Capitalismo de Vigilância: o Caso de *Palantir Technologies Inc.* em análise (2001-2023)

Universidade do Minho
Escola de Economia e Gestão





Universidade do Minho

Escola de Economia e Gestão

Patrícia Alexandra Gonçalves Névoa

**Capitalismo de Vigilância: o Caso de
Palantir Technologies Inc. em análise
(2001-2023)**

Dissertação de Mestrado

Relações Internacionais

Trabalho efetuado sob a orientação da

**Professora Doutora Alena Vysotskaya Guedes
Vieira**

outubro de 2024

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição-NãoComercial
CC BY-NC

<https://creativecommons.org/licenses/by-nc/4.0/>

Agradecimentos

À minha família, um especial agradecimento pelo apoio, suporte e por toda a paciência.

Aos meus amigos, agradeço pelas palavras de motivação.

À minha orientadora, Professora Doutora Alena Vysotskaya Guedes Vieira, um especial agradecimento pela confiança depositada em mim e por me ajudar a manter o foco e o rigor no desenvolvimento da dissertação.

Ao Fábio, por me ouvir, por me ajudar a descomplicar o processo de investigação e por me trazer à razão nos momentos cruciais.

Ao Santiago, um reconhecimento especial, pois a sua presença alegre e inocente trouxe momentos de alívio e serenidade durante os períodos mais intensos.

O meu agradecimento vai para além das palavras aqui escritas.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Capitalismo de Vigilância: o Caso de *Palantir Technologies Inc.* em análise (2001-2023)

Resumo

A era digital vivenciada no século XXI tem determinado uma nova realidade associada à propagação do fenómeno *BigData*. Este contexto está assente numa incessante lógica de acumulação de uma vasta diversidade e quantidade de metadados, de dados pessoais e de informações pessoais identificáveis. A acumulação é realizada por atores institucionais e por empresas privadas, através da chamada - vigilância massificada de dados -. Por conseguinte, esta última tem originado um lucro de tal ordem notável que se reflete numa versão capitalista deste tema, à qual Shoshana Zuboff atribuiu o nome - capitalismo de vigilância -, abordagem teórica condutora do desenvolvimento da presente dissertação.

A recente versão do capitalismo, associada à vigilância massificada de dados, foi legitimada pela necessidade de uma cooperação entre atores das Relações Internacionais, o Estado e o setor privado, considerando a emergência na prevenção de ataques semelhantes aos ataques terroristas efetuados a 11 de setembro de 2001. Para a presente investigação, é analisada em detalhe, através de uma metodologia qualitativa e da análise de um estudo de caso, a cooperação entre a empresa *Palantir Technologies Inc.* e as seguintes unidades de segurança dos Estados Unidos da América (EUA): o Departamento da Polícia de Los Angeles, o Departamento da Polícia de Nova Orleães, e a agência governamental de Imigração e Fiscalização Aduaneira dos EUA, analisadas individualmente.

Como tal, o principal objetivo desta dissertação é perceber em que enquadramento surge a fusão do Estado com o setor privado, relativamente à utilização dos dados da população, no campo referido, respondendo ainda à seguinte pergunta de investigação: “Como se tem desenvolvido a interação do Estado com o setor privado num contexto de *policing*, em matéria de vigilância e utilização de dados?”.

A dissertação vem demonstrar como se tem desenvolvido esta cooperação, tendo por base documentação que contém informação sobre o período vivido entre 2001 e 2023. A escolha do ano de 2001, justifica-se pela importância que o período pós-11 de setembro teve nas opções securitárias dos EUA. O ano de 2023, por ser o ano do término da exploração do estudo de caso.

Palavras-chave: Capitalismo de Vigilância; Cooperação; Dados; EUA; *Palantir Technologies Inc.*; 11 de setembro

Surveillance Capitalism: the case of Palantir Technologies Inc. under analysis (2001-2023)

Abstract

The digital age experienced in the 21st century has led to a new reality associated with the proliferation of the BigData phenomenon. This context is based on the incessant logic of accumulation of a vast diversity and quantity of metadata, personal data and personally identifiable information. This accumulation is carried out by institutional actors and private companies through what is known as - mass data surveillance -. As a result, the latter has generated such a remarkable market profit that it is reflected in a capitalist version of this issue, to which Shoshana Zuboff has named - surveillance capitalism -, the theoretical approach guiding the development of the present dissertation.

The recent version of capitalism, associated with mass data surveillance, has been legitimized by the need for cooperation between actors in International Relations, the state and the private sector, considering the emergency in preventing attacks similar to the terrorist attacks carried out on September 11, 2001. For this research, the cooperation between the company Palantir Technologies Inc. and the following security units in the United States of America (USA) is analyzed in detail, through a qualitative methodology and the analysis of a case study: the Los Angeles Police Department, the New Orleans Police Department, and the US government agency Immigration and Customs Enforcement, analyzed individually.

As such, the main objective of this dissertation is to understand the framework in which the merger between the state and the private sector arises, in relation to the use of population data, in the aforementioned field, and to answer the following research question: "How has the interaction between the state and the private sector been developing in a policing context, in terms of surveillance and use of data?".

The dissertation demonstrates how this cooperation has been developing, based on documentation containing information on the period between 2001 and 2023. The year 2001 was chosen because of the importance that the post-9/11 had on US security choices. The year 2023, as it is the year in which the research for the case study ended.

Keywords: Surveillance Capitalism; Cooperation; Data; USA; Palantir Technologies Inc.; September 11th

Índice

Introdução	12
1. Identificação e relevância temática	12
2. Revisão da bibliografia	14
2.1. Ascensão do setor privado	15
2.2. O novo papel do Estado no domínio do digital, despertado no período pós-11 de setembro	18
2.3. Alteração da ótica de poder: a necessidade de cooperação entre o Estado e o setor privado	21
3. Perspetiva Metodológica	27
3.1. Epistemologia e Ontologia	27
3.2. O estudo de caso	28
3.3. Tipo de estudo de caso	29
4. Métodos e Recolha de dados	30
5. Estrutura da dissertação	31
Capítulo I. Abordagem teórica: o capitalismo de vigilância	33
1.1. Tecnologias de segurança e o ‘complexo industrial de segurança’	33
1.1.1. ‘Complexo industrial de segurança’	36
1.2. Capitalismo de vigilância: uma visão geral	38
1.3. As principais características do capitalismo de vigilância	41
1.4. Os imperativos que sustentam o capitalismo de vigilância	44
1.4.1. O imperativo de extração e as economias de escala	44
1.4.2. O imperativo de previsão e as economias de âmbito	45
1.4.3. O imperativo de previsão e as economias de ação	46
1.5. Os 16 fatores impulsionadores do capitalismo de vigilância	49
1.6. O poder ‘instrumentarista’ do capitalismo de vigilância	55
Capítulo II. A nova conjuntura (inter-)nacional e a emergência de <i>Palantir Technologies</i>	58
2.1. A nova conjuntura (inter-)nacional: 11 de setembro e o advento do intelligence-led policing	58
2.2. A emergência de Palantir Technologies: uma visão geral	64
Capítulo III. Imperativos do capitalismo de vigilância na cooperação entre EUA e <i>Palantir Technologies</i>	70
3.1. A cooperação de Palantir Technologies com Departamentos da Polícia dos EUA	70

3.1.1. A cooperação de <i>Palantir Technologies</i> com o Departamento da Polícia de Los Angeles: A operação <i>LASER</i>	70
3.2.2. A cooperação de <i>Palantir Technologies</i> com o Departamento da Polícia de Nova Orleães.....	84
3.3. A cooperação de Palantir Technologies com a agência: Imigração e Alfândega dos EUA (ICE).....	99
3.3.1. Plataforma <i>Investigative Case Management (ICM)</i> na cooperação com <i>Palantir Technologies</i>	99
Conclusão.....	110
Anexos.....	120
Anexo I - Software enquanto serviço – produto Apollo de Palantir Technologies	121
Anexo II - Rede de contactos estabelecida e visualizada através do software de Palantir Technologies	122
Anexo III – Exemplo de uma carta enviada a um infrator reincidente	123
Anexo IV – Utilização da estratégia: análise de redes/interações sociais.....	123
Anexo V – A “caixa-negra” nos sistemas de aprendizagem automática.....	124
Anexo VI – Relação contratual entre Palantir Technologies e a agência ICE	125
Anexo VII –Bases de dados a que é possível aceder a partir da plataforma ICM	126
Anexo VIII – Os sistemas de gestão de processos da agência ICE e a sua rede contratual ..	127
Anexo IX – Rede de elementos que sustentam a atividade da agência ICE	128
BIBLIOGRAFIA:.....	129
Entrevista:	129
Fontes Primárias:.....	129
Fontes secundárias:.....	132

Índice de Figuras e Tabelas

Figura 1. Três correntes da bibliografia. (Criação livre da autora).	15
--	----

Tabela 1. Objetivos declarados versus a ação dos departamentos de Los Angeles e Nova Orleães: assegurar a segurança pública com novas ferramentas de predictive policing. (Criação livre da autora).	118
--	-----

Tabela 2. Categorias de análise do Capitalismo de Vigilância de Shoshana Zuboff. (Criação livre da autora).	119
---	-----

Lista de Abreviaturas

ALPR	The Automatic License Plate Reader
CIA	Central Intelligence Agency
DHS	Department of Homeland Security
DICFP	Data-Informed Community-Focused Policing
ERRO	Enforcement and Removal Operations
EUA	Estados Unidos da América
FBI	Federal Bureau of Investigation
HIS	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
ICM	Investigative Case Management
JRIC	Joint Regional Intelligence Center
DPLA	Departamento da Polícia de Los Angeles
DPNO	Departamento da Polícia de Nova Orleães
NOLA	Nova Orleães, Louisiana
NSA	National Security Agency
NYSE	New York Stock Exchange
OIG	Office of the Inspector General
OSLLE	The Office for State and Local Law Enforcement
PLTR	Palantir (abreviação na Bolsa de Valores de Nova Iorque (NYSE))

Introdução

1. Identificação e relevância temática

O principal foco desta dissertação centra-se na análise do fenómeno de fusão entre o Estado e as empresas privadas, no que diz respeito à vigilância dos dados dos cidadãos, o que constitui um *surveillance-industrial complex* (complexo de uma indústria de vigilância)¹, bem como as suas implicações.

A análise desta dissertação incidirá sobre a empresa *Palantir Technologies*, sediada nos EUA e sobre a sua cooperação com o referido país, mais concretamente com os Departamentos da Polícia de Los Angeles e da Polícia de Nova Orleães e com a Agência Governamental de Imigração e Fiscalização Aduaneira (*ICE*)², analisadas individualmente. A análise será realizada sob a abordagem teórica do Capitalismo de Vigilância de Shoshana Zuboff (2019). Assim, a pergunta de investigação que se procura responder nesta dissertação é: “Como se tem desenvolvido a interação do Estado com o setor privado num contexto de *policing* e controlo da imigração, em matéria de vigilância de dados?”.

A presente dissertação visa debruçar-se sobre um tópico de pesquisa atual, a vigilância de dados, especialmente pertinente no mundo digital contemporâneo, marcado pela tecnologia. A esta relevância temática, acresce a pertinência do tema para a sociedade, tendo em conta a crescente importância do argumento dos dados serem o novo petróleo. A relevância da dissertação prende-se ainda com o facto de abordar a problemática que se apresenta com a ameaça à privacidade e à proteção de dados, devido à natureza sigilosa da cooperação entre o Estado e o setor privado num contexto de *policing*. Além disto, a presente dissertação, ao dissecar a cooperação já mencionada, salienta a lógica capitalista associada à vigilância de dados uma vez que, por um lado, verifica-se a angariação de lucros por parte das empresas privadas, através de contratos com o Estado e, por outro, verifica-se a angariação por parte deste de uma coleção

¹ Antes de dar início à introdução importa referir, que todo o trabalho de estudo, análise, reflexão e conclusão é baseado em documentos associados aos Estados Unidos da América (EUA), pelo que a sua língua original é a língua inglesa. Assim, e uma vez que os próprios acontecimentos e evoluções obrigaram, foram criados termos técnicos associados a esta temática que passaram, por si só, a ter um significado específico nem sempre traduzível para outras línguas. Consequentemente, esses termos técnicos são usados noutros países sem a necessidade de serem constantemente traduzidos. Aqui, sempre que possível, serão explicados sucintamente para facilitar a compreensão da leitura.

² *ICE* é o acrónimo da agência governamental dos EUA - *Immigration and Customs Enforcement* - que nesta dissertação é traduzido para- agência governamental de Imigração e Fiscalização Aduaneira. Apesar da tradução ser apresentada, o acrónimo original, *ICE*, será a escolha ao longo da dissertação, pois é facilmente identificável e amplamente reconhecido, o que facilita também a leitura.

³ O termo *policing* é usado na presente dissertação em inglês, pois a sua tradução para português – policiamento - não reflete na totalidade as componentes envolvidas na investigação: “(...) the practice of community policing by the nation’s state, local, territorial, and tribal law enforcement agencies through information, technical assistance, training and grant resources (...), comprising key operational divisions and several functional áreas.” (Departamento de Justiça dos EUA s.d.)

insólita de dados acerca da população sem que haja a necessidade de obtenção de um mandado judicial. Por fim, a relevância e importância do tema escolhido prende-se, também, pelo facto de trazer à discussão a falta de conhecimento e escrutínio público que existe perante esta cooperação no contexto de *policing* e as repercussões jurídicas que daí podem surgir para a população. Importa referir que esta última dimensão se revela fundamental tendo em consideração a preocupação em compreender quais são os dados que estão a ser utilizados, de que forma ou com base em que parâmetros estão a ser recolhidos, e quem ou para que efeitos estão a ser utilizados.

Deste modo, pretende-se com a presente investigação, trazer um contributo social no sentido de alertar a sociedade sobre os potenciais perigos relacionados com a vigilância em massa dos dados dos cidadãos. Estes perigos são muitas vezes ocultados tanto pelas empresas, que se apoiam no discurso da inevitabilidade enquanto retiram os benefícios de um mundo tecnológico, como pelo Estado que recorre ao discurso securitário, como por exemplo, ao sublinhar a influência duradoura dos ataques terroristas de 11 de setembro de 2001, elevando a sobreposição da segurança nacional a questões de privacidade.

Além da relevância subjacente à investigação, esta dissertação visa produzir um contributo original, que resulta da aplicação da abordagem teórica do Capitalismo de Vigilância a um estudo de caso em particular, *Palantir Technologies*, que ainda não existe na extensa e crescente bibliografia⁴ sobre o tema de vigilância dos dados. A abordagem escolhida permite ainda, mesmo que de modo subsidiário, refletir sobre o papel do Estado na nova dinâmica de mercado e na inovadora forma de atuação.

A baliza temporal deste estudo é determinada pelos acontecimentos que tiveram início em 2001 e que terminaram em 2024. Destaca-se o evento de 11 de setembro de 2001, uma vez que representou um ponto de viragem para as políticas de segurança dos EUA, com a aceleração no desenvolvimento e implementação de diretivas de combate ao terrorismo, e numa crescente aproximação às empresas privadas na procura pelas suas capacidades analíticas.

⁴ Durante a apreciação da bibliografia, não foram encontradas referências a um estudo de caso que combinasse reflexões sobre estudos de segurança, reflexões sobre as consequências dos acontecimentos de 11 de setembro de 2001 (e a sua influência na evolução da vigilância dos dados dos indivíduos) e reflexões sobre o fenómeno *BigData*. A título ilustrativo, apresenta-se de seguida os resultados da pesquisa na *Web of Science*, sobre a combinação destes 3 temas, onde é possível verificar a inexistência de documentos com a combinação pretendida. Os resultados surgem na sequência do uso dos critérios de pesquisa seguintes:

Social Sciences Citation Index (collection), filtro:

1 - "surveillance capitalism" (field 1 – abstract) + "Palantir Technologies Inc." (field 2 – abstract) – 0 resultados

2 - "surveillance capitalism" (field 1 – abstract) + "Palantir Technologies Inc." (field 2 – abstract) + "security studies" (field 3 – abstract) + "BigData" (field 4 – abstract) – 0 resultados

3 - "surveillance capitalism" (field 1 – abstract) + "Palantir Technologies Inc." (field 2 – abstract) + "security studies" (field 3 – abstract) + "BigData" (field 4 – abstract) + "state and market cooperation" (field 5 – abstract): 0 resultados.

2. Revisão da bibliografia

Antes de prosseguir com a revisão da bibliografia, é importante destacar a interdisciplinaridade do tópico de investigação analisado nesta dissertação, que vem aumentar a complexidade do estudo. O estudo sobre vigilância e proteção de dados é comum a várias disciplinas de estudo das Ciências Sociais como Ciência Política, Sociologia, Direito e Economia. Da bibliografia fazem parte autores que se incluem nas disciplinas acima referidas. A saber, Ronald J. Deibert com “*Black Code: Surveillance, Privacy, and the Dark Side of the Internet*” (2013) na Ciência Política; Shoshana Zuboff com “*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*” (2019) na Sociologia; Lawrence Lessig com “*Code: And Other Laws of Cyberspace*” (1999) e Frank Pasquale com “*The Black Box Society: The Secret Algorithms That Control Money and Information*” (2015) no Direito e Catherine Tucker com “*The Economics of Advertising and Privacy*” (2012) na Economia. O tema primordial desta dissertação está a crescer também no campo das Relações Internacionais, com artigos, como por exemplo, de Daniel W. Drezner com “*The Irony of Global Economic Governance: The System Worked*” (2012) e David Murakami Wood com “*Globalization and Surveillance: The Watched World*” (2015). Assim, a disciplina das Relações Internacionais está a dar os primeiros passos no que respeita à sua contribuição para o estudo da vigilância de dados. Consequentemente, as grandes teorias das Relações Internacionais, como o realismo, o construtivismo e o institucionalismo liberal ainda não foram aplicadas ao estudo. É, então, por esse motivo que esta dissertação almeja enriquecer a pesquisa sobre este tópico, no campo das Relações Internacionais, ainda que sob o ponto de vista de uma abordagem teórica recente – o capitalismo de vigilância.

Ao explorar a bibliografia foi possível identificar as principais correntes que comportam o estudo: a corrente económica, aqui denominada por “Ascensão do setor privado”, quando fala do papel dominante das empresas em traçar o alinhamento do mercado; a corrente associada aos estudos de segurança, aqui denominada “O novo papel do Estado no domínio do digital, despertado no período pós-11 de setembro”, estudos esses que refletem sobre os ataques terroristas de 11 de setembro de 2001, enquanto elemento-chave na alteração do papel do Estado no digital; e a corrente que aborda as novas capacidades analíticas associadas ao setor privado, aqui denominada por “A alteração da ótica de poder: a necessidade de cooperação entre o Estado e o setor privado”, nomeadamente empresas tecnológicas e de software, que impelem a interação entre o Estado e o setor privado.

De modo a facilitar a compreensão das correntes identificadas, associadas ao tema em questão, apresenta-se o esquema seguinte:

Correntes presentes na bibliografia:

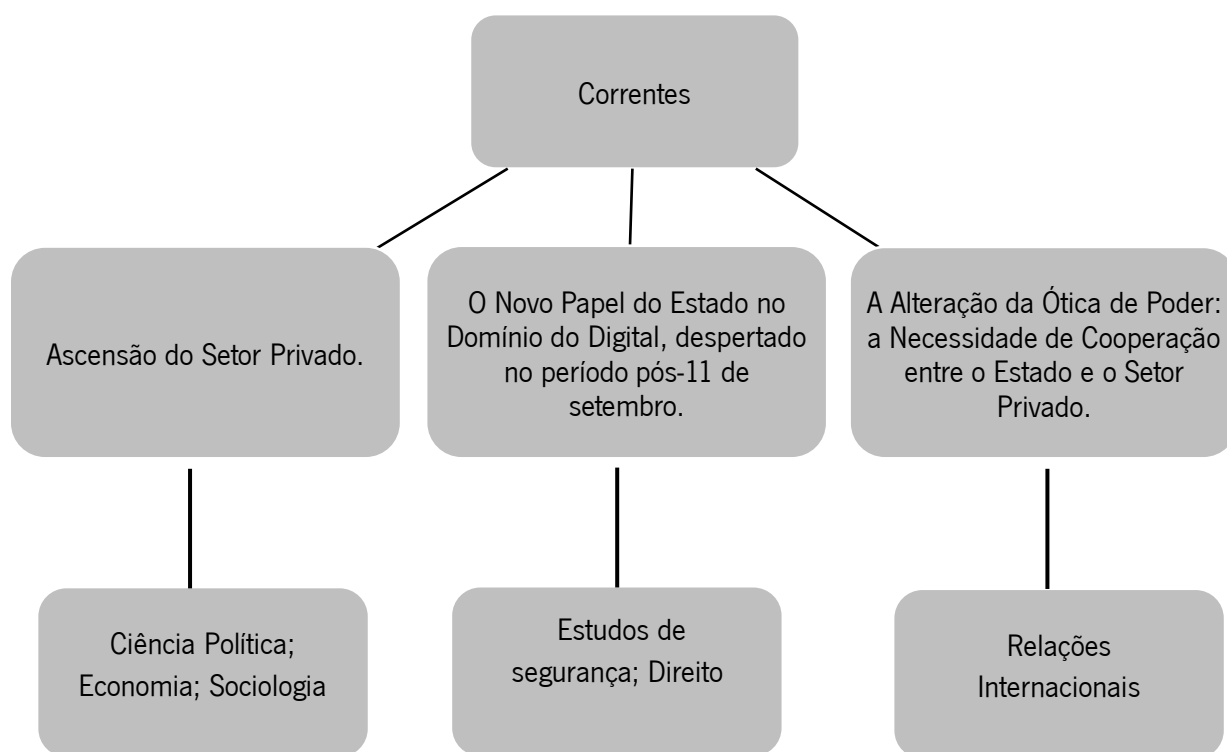


Figura 1. Três correntes da bibliografia. (Criação livre da autora).

2.1. Ascensão do setor privado

Na primeira corrente identificada – Ascensão do Setor Privado – a bibliografia reflete sobre o crescente desenvolvimento do setor privado, nomeadamente de empresas tecnológicas e de software, e sobre a adoção de métodos e análises preditivas a partir da exploração dos dados, notadamente a partir do desenvolvimento de *BigData*. Assim, o setor privado tornou-se capaz de fazer uma análise de riscos e preferências da população a partir dos dados da última, passando estes a servir interesses alheios a si. Estas empresas acabam por atingir receitas crescentes em malefício do direito sobre os dados pessoais (Olesen 2022; Landwehr, Borning e Wulf 2021; Connor e Doan 2021; Zuboff 2019).

Quando se fala em *BigData*⁵, a bibliografia não se refere apenas ao volume de dados e à velocidade com que os mesmos se geram, mas também à sua variedade, o que compõe a complexidade e capacidade dos sistemas analíticos que tratam estes dados (Puyvelde, Coulthart e Hossain 2017).

Os métodos analíticos de *BigData*⁶ são também salientados na bibliografia. Não obstante, a ênfase não é dada aos métodos tecnológicos por si só, nem aos analistas das empresas que vão contextualizar esta informação. A ênfase é dada ao trabalho conjunto entre a tecnologia e a capacidade humana de contextualizar a análise fornecida pela primeira. O objetivo deste trabalho conjunto é não gerar falsos resultados positivos (Puyvelde, Coulthart e Hossain 2017). No entanto, uma vez que o papel do analista é reforçado na bibliografia, não se deve esquecer que o ser humano pode fazer escolhas parciais e inviáveis de acordo com a sua interpretação. Consequentemente, na bibliografia, é dado um alerta a este poder significativo das tecnologias e das suas análises preditivas (interpretadas pelo ser humano), por terem sido introduzidas e combinadas novas abordagens e critérios de análise, uma vez que essas análises preditivas, sobre aspetos que envolviam a sociedade e o seu quotidiano, passaram a ser incorporadas nas tomadas de decisão das instituições.

Tal como Damien Van Puyvelde, Stephen Coulthart e M. Shahriar Hossain (2017) explicam, a tecnologia das empresas veio substituir muito a capacidade humana em termos de previsão e análise de comportamentos de pessoas, utilizadores e compradores, angariando para si o poder de previsão. Ainda assim, sempre que se trabalha a questão dos dados, é necessário haver coordenação entre a tecnologia e o ser humano pois é a tecnologia que regista e faz o cruzamento dos vários dados e que gera informação analítica e, é o ser humano que interpreta e contextualiza a informação obtida. A título de exemplo, ao serem trabalhados dados na

⁵ O conceito de *BigData* surge com a evolução das tecnologias e foi sendo abordado e desenvolvido ao longo do tempo. Hoje, este termo, *BigData*, é hermetico devido ao complexo digital envolvente, isto é, envolve um conjunto de sistemas de análise de dados que retiram informação e análises estatísticas desses dados.

Dentro da bibliografia, a definição menos técnica do que é *BigData* traduz-se na seguinte: “(...) os ativos de informação caracterizam-se por um volume, velocidade e variedade tão elevados que exigem tecnologias e métodos analíticos específicos para a sua transformação em valor.” Estas tecnologias e métodos analíticos contribuíram para o desenvolvimento das redes sociais, para o desenvolvimento de serviços de *cloud computing*, de armazenamento de dados e ainda, para o desenvolvimento de uma conectividade móvel caracterizada pela dependência (Mauro et al. citado por Puyvelde, Coulthart, e Hossain 2017).

Estas quantidades volumosas de dados obtidas a partir da população é, através da utilização diária e incessante dos telemóveis, computadores, televisores, relógios, carros, aplicações *smart*, registada e processada por um complexo de sistemas “inteligentes” que facilitam a rápida captação e análise detalhada desses dados (Landwehr, Borning, e Wulf 2021).

⁶ Com a evolução das tecnologias, a partir do século XXI, e com a descoberta e utilização do fenómeno de *BigData* para a atividade lucrativa das empresas desenvolveu-se um conjunto complexo de métodos e técnicas que visavam assegurar às empresas, e posteriormente aos Estados, o contínuo acesso a dados sem qualquer tipo de restrição. Para além disto, com a evolução das capacidades algorítmicas e analíticas de software das empresas foi possível para estas transformar o fenómeno de *BigData* na construção e visualização de comportamentos e escolhas futuras dos utilizadores.

identificação da origem de ciberataques, na identificação de redes criminosas, na antecipação de crimes, na identificação de identidades terroristas, é sempre necessário haver coordenação entre a tecnologia e o ser humano, para evitar injustiças e erros.

Os métodos de análise de dados comportam ainda os chamados algoritmos. Estes, para além de servirem para extrair informação, a chamada *data-mining*, servem também, para aumentar o lucro das empresas. Estes objetivos dos algoritmos são-lhes atribuídos, no momento em que são criados, de acordo com a orientação económica pretendida. Os algoritmos são criados através da identificação das preferências dos utilizadores/consumidores, designada por *personalized information* (informação personalizada), e da exposição dos seus produtos. “Os algoritmos são também utilizados para procurar padrões, que serão utilizados pelos computadores para ajustar ações de programas específicos (...), num processo denominado ‘treino’, e ajusta os seus algoritmos para atribuir valores ou categorias a exemplos não rotulados.” (Puyvelde, Coulthart e Hossain 2017, 1408-1409)⁷.

Empresas como a Microsoft, a Google, a Amazon, a Apple, o Facebook (Meta) e o Twitter, determinam muito do conteúdo e da variedade que se encontra no domínio do digital. Esta determinação permite-lhes aumentar a sua afluência e a preferência das pessoas pelas suas plataformas e produtos, o que gera toda a sua soberania no ciberespaço, relativamente a outras empresas. Assim, as grandes empresas servem-se dos métodos de análise de dados para garantir a sua soberania.

A perceção de que seria possível transformar os dados em lucro, levou as empresas a procurar, de forma exacerbada, todas as rotas que levassem à obtenção de um maior e melhor acesso a dados. Ao mesmo tempo, encontraram formas de proteger e assegurar essas mesmas rotas. As empresas perceberam que através da vigilância massificada seria possível aumentar o seu poder económico e financeiro, promovendo assim o capitalismo económico.

A vigilância massificada e os mecanismos a ela associados são interpretados como um novo fenómeno, estudado pela autora Shoshana Zuboff. A análise deste fenómeno permitiu-lhe identificar uma nova dinâmica do capitalismo, que integrava novos imperativos económicos, à qual a autora denominou Capitalismo de Vigilância. Shoshana Zuboff traçou o caminho e identificou os vários fatores que fizeram chegar até à dinâmica capitalista que se vive hoje. Shoshana Zuboff refere que o fator determinante para esta nova lógica de acumulação, foi o momento de crise de

⁷ Tradução livre de: Algorithms are also used to look for patterns that will be used by computers to adjust specific programs actions (...) in a process called “training”, and adjusts its algorithms to assign values or categories to unlabelled examples.

uma das maiores empresas tecnológicas, a Google, em 2002, quando os lucros não estavam a ser suficientes, tendo em conta o investimento realizado. Esta identificação de momentos de crise, como fatores que desencadeiam medidas extraordinárias que se prolongam no tempo, é muito comum entre a bibliografia (Zuboff 2019; Véliz 2022).

Ao realizar o estudo sobre toda a bibliografia percebe-se que esta vigilância por parte das empresas é um método ilegítimo de extração, análise e utilização dos dados da população, para produzir o *targeted advertising* (publicidade diretamente direcionada), com o claro objetivo de levar os utilizadores a comprar os seus produtos. Os atores privados exploram, gradualmente, a possibilidade de modificar os comportamentos da população em direção aos seus objetivos, sendo estes alheios à própria população. Isto é, o setor privado, por meio do *digital profiling* (criação do perfil do utilizador no domínio do digital), prevê comportamentos e tenta modificá-los, de acordo com os seus objetivos.

Em conclusão, o desejo de aumentar o lucro e o crescimento destas companhias é central para as mesmas uma vez que, corresponde à sua sobrevivência no mercado, mas, nota-se que, fica em esquecimento o valor humano e a vontade dos utilizadores/consumidores (Landwehr, Borning e Wulf 2021, 74).

A população que consome os serviços e produtos destas empresas, em geral não tem a perceção de que os dados estão a ser extraídos, registados, arquivados e analisados para promover o lucro destes capitalistas. Percebe-se, por uma questão económica, que este capitalismo de vigilância é uma prática realizada em massa por estas empresas e incorre no quotidiano da população, uma vez que os principais aspetos da vida em sociedade estão, de alguma forma, associados ao domínio do digital. Tal como nos confirmam, na bibliografia, Landwehr, Borning e Wulf: “Os *loci* de controlo atualmente dominantes são, principalmente, os serviços gratuitos das redes sociais e de navegação na *Internet*. Estes são simultaneamente o campo de batalha e as armas com que os capitalistas de vigilância lutam pela sua influência.” (Landwehr, Borning e Wulf 2021, 73)⁸.

2.2. O novo papel do Estado no domínio do digital, despertado no período pós-11 de setembro

⁸ Tradução livre de: The currently dominant loci of control can be considered to be mainly the free services of social media and browsing. They are both the battlefield and the weapons with which surveillance capitalists fight for influence.

Na segunda corrente identificada – O novo papel do Estado no domínio do digital, despertado no período pós-11 de setembro – a bibliografia debruça-se sobre a corrente de pensamento que reflete sobre o 11 de setembro e o despertar do novo papel do Estado no digital. Esta corrente enquadra-se nos estudos de segurança, que identificam os acontecimentos desse dia como peça-chave no desbloquear de uma nova ação do Estado, perante a segurança na procura pela supervisão do novo domínio do digital (Damin 2013; Deibert 2020; Pohle e Van Audenhove 2017; Pohle e Thiel 2020; Puyvelde, Coulthart e Hossain 2017).

Os acontecimentos de 11 de setembro de 2001 marcaram as Relações Internacionais e mostraram ao mundo que nem os EUA, outrora potência hegemónica num sistema unipolar, conseguiram prever e defender-se de ataques como aqueles. A falha no sistema de segurança norte-americano deveu-se à falta de ligação da *intelligence* (refere-se à compreensão das relações, padrões, tendências e implicações da informação para fazer previsões, interpretações e recomendações através de análises de risco, métricas de desempenho e estratégias com a aplicação de métodos de extração de dados e aprendizagem automática (Jacky s.d.)) entre as várias agências de segurança do aparelho securitário dos EUA. Identificada a falha, deu-se uma mudança significativa nas prioridades securitárias do país, o que podemos confirmar nas palavras de Deibert, “Após o 11 de setembro sucedeu-se também uma mudança no pensamento militar dos EUA que afetou profundamente o ciberespaço. A definição de ciberespaço enquanto domínio único - igual a terra, mar, ar e espaço – foi formalizada no início dos anos 2000, criando o imperativo para dominar e governar este domínio (...)”. (Deibert 2015, 11)⁹.

Os EUA, país de análise na investigação, enfraquecidos pela ideia de falhanço e pelo medo, começaram a investir no ciberespaço, mais concretamente na procura pela soberania do digital. O investimento baseou-se em questões de segurança, pois pretendiam ser capazes de antecipar e, conseqüentemente, travar ataques terroristas como o de 2001. Desta forma, começou a assistir-se, com maior expressão, à vigilância da população no digital, agora por parte do Estado.

Cláudio Damin complementa o argumento ao explicar que os próprios Estados começaram a incorrer sobre o digital, num apelo à segurança nacional. Mas, a segurança nacional implicaria a vigilância de todos os aspetos da vida social da população-alvo, sem que a mesma tivesse esse conhecimento. A segurança nacional comprometeu as liberdades e os direitos individuais (Damin 2013, 33).

⁹ Tradução livre de: After 9/11, there was also a shift in US military thinking that profoundly affected cyberspace as a single 'domain' – equal to land, sea, air, and space – was formalized in the early 2000s, leading to the imperative to dominate and rule this domain (...).

É, a partir deste ponto, que se assiste à transformação do papel do Estado, iniciada a partir da criação de condições favoráveis para a contínua vigilância, suportada e facilitada pelas empresas tecnológicas, que a fazem de forma eficaz devido às suas capacidades inerentes. O que os Estados começaram também a perceber, com o digital, foi o facto de que, em pleno século XXI, eram outros a deter soberania sobre um domínio que cobria, nesse momento, todos os aspetos da vida humana. Apercebendo-se do potencial desse novo espaço comunitário, os Estados procuraram também ganhar a sua soberania digital. No entanto, hoje, os Estados entendem que para ter um controlo maior sobre este domínio e, para melhor dar resposta às suas questões de segurança, necessitam do setor privado para o fazer (Pohle e Thiel 2020, 2).

Por outro lado, apresentava-se ali uma oportunidade para as empresas, através do *lobbying* (lôbi), conseguirem ver consagrados os seus imperativos económicos, sem a constante ameaça de uma crescente legislação do ciberespaço: “O ciberespaço não é imune à política. A convicção popular de que o ciberespaço pode ser uma utopia libertária parece totalmente irrealista.” (Liaropoulos 2016, 22)¹⁰.

Os imperativos económicos exigiam, então, vigilância constante de dados. Esta vigilância transformou-se em hipervigilância, sem controlo que lhe fosse associado. Ainda assim, verifica-se, na bibliografia, um conjunto de relatos de denúncias sobre casos de hipervigilância, contra as empresas e contra o Estado, como por exemplo os casos “*Supercookies: corporate invasions of privacy*.” e “*NSA surveillance: the villainous state?*” (Conor e Doan 2021, 57; 61), respetivamente. Contudo, relatos sobre a interação entre os casos de hipervigilância denunciados foram pouco sustentados academicamente com estudos de caso que nos comprovem a relação entre a hipervigilância efetuada pelo Estado e pelo setor privado. Apesar de existirem artigos mencionados neste trabalho de investigação que retratam a interação entre EUA e a empresa *Palantir Technologies*, não reconsideram o papel do Estado na atual conduta de mercado – lógica do capitalismo de vigilância. Na bibliografia, temos o contributo de Knight e Gekker (2020), que incide sobre a cooperação¹¹ entre a agência ICE e *Palantir Technologies*. Ainda que o artigo aponte para a problemática da cooperação entre Estado e setor privado, e para a dependência do Estado para

¹⁰ Tradução livre de: Cyberspace is not immune to politics. The popular belief that cyberspace can be a libertarian utopia seems utterly unrealistic.

¹¹ Apesar de, na bibliografia, haver estudos sobre a empresa *Palantir Technologies* e a sua ação junto de agências governamentais, não é analisado também o novo papel e poder do Estado na cooperação público-privada, no que respeita à vigilância em massa dos indivíduos. Ambos os atores, Estado e empresas privadas, conseguem ter um conhecimento sobre a sua população que a própria não tem, nem se apercebe que existe. Este desconhecimento por parte da população permite ainda que o Estado e o setor privado prevejam e antecipem os seus movimentos e escolhas. Existe, então, assimetria do conhecimento entre os que detêm o poder e os cidadãos, que se vem desenvolvendo por meio da presente dinâmica de mercado. Esta assimetria ajuda a deliberar que a interação entre o Estado e o setor privado tem, muitas vezes, consequências para os direitos e liberdades individuais.

com a elite tecnológica para assegurar o seu aparelho de segurança, não trata a mecânica da cooperação nos campos de *policing* e controlo da imigração, algo que a presente dissertação pretende analisar:

“Ao recorrer à indústria privada para construir o aparelho moderno de segurança dos Estados Unidos, a securitização nunca foi tratada como uma questão política, mas sim como um problema técnico que só poderia ser resolvido pelo poder das melhores mentes do setor privado. Por sua vez, os contratantes privados desenvolveram, construíram e mantiveram eficazmente as atuais infraestruturas de vigilância e segurança tecnológica do país.” (Knight e Gekker 2020, 234)¹².

2.3. Alteração da ótica de poder: a necessidade de cooperação entre o Estado e o setor privado

Na terceira corrente identificada – Alteração da ótica de poder: a necessidade de cooperação entre o Estado e o setor privado – será analisada a alteração que existe, na perspetiva dos autores, no poder do Estado. Como consequência do desenvolvimento da tecnologia e de novos tipos de ameaças, o Estado compreendeu a necessidade de uma melhor cooperação com as empresas, de forma a dar resposta às suas necessidades e às da população nacional (Strange 1995; Strange 1998; Tooze 2010).

Nesta revisão do estado da arte é importante refletir sobre o trabalho científico de Susan Strange e o seu enquadramento. Note-se que, Susan Strange é uma autora associada às Relações Internacionais, mais concretamente à Economia Política Internacional, pelo que o seu foco incidiu na alteração dos detentores do poder ao longo do tempo e na complementaridade entre esses detentores. Referir Relações Internacionais e Susan Strange obriga a referir Economia Política Internacional e Guerra e Paz. Assim é imperativo abordar nesta dissertação, já de seguida, todo um conjunto de temas que aparentemente não se relacionam com o tema central da dissertação – vigilância de dados – mas que mais tarde serão conectadas ao mesmo.

As relações de poder fazem parte das Relações Internacionais e continuam a estar na mesa de discussão das grandes salas da cena internacional. Na maioria das vezes têm como

¹² Tradução livre de: By turning to private industry to build America's modern security apparatus, securitization was never treated as a political issue but rather as a technical problem that could only be solved by "the power of the best minds of the private sector" (...). In turn, private contractors have effectively developed, built, and maintained the country's current surveillance and technological security infrastructures.

consequência a dicotomia guerra/paz. No entanto, a autora considera que as relações de poder abrangem áreas que nem sempre conduzem a guerra. Assim, alerta para o facto de que a guerra e a paz não deverão ser as únicas problemáticas determinantes presentes nas Relações Internacionais. As relações de poder entre Estado e setor privado também deverão constar da sua lista de preocupações.

No trabalho de Susan Strange existe uma ligação entre as áreas da economia e da política, por serem essas as suas áreas de pesquisa. Segundo a autora, estas áreas não se desvinculam uma da outra, ao contrário do que acontece nos grandes paradigmas das Relações Internacionais. Ao analisar a lógica de poder, a autora acrescenta ainda que a análise das políticas internacionais não se deve afastar da análise das políticas domésticas. Estas opiniões estão refletidas nas suas palavras: “(...) a essência do realismo, tal como o entendo, é o reconhecimento de que os resultados, mesmo em matéria de comércio e finanças, não podem ser corretamente analisados (...) sem levar em conta a distribuição do poder.” (Susan Strange citada por Tooze 2010, 284)¹³.

Susan Strange acaba por mostrar que existe uma vertente, na lógica de poder, que vai mais longe relativamente ao comum conceito de poder em Relações Internacionais. O seu novo conceito de poder inclui as relações de poder entre Estado e setor privado. Strange acrescenta esta vertente ao constatar que foram certas estruturas globais como a integração do crédito, que determinaram e determinam, para além da lógica de acumulação, o sistema de capital que começamos a viver há cerca de duas décadas. O aparecimento deste sistema de capital, deve-se, segundo a autora, às mudanças trazidas pelas tecnologias. Assim, num plano geral sobre capitalismo económico, é até possível fazer associação e referência aos seguidores do marxismo pois estes referem a acumulação de poder e riqueza como a característica principal da dinâmica capitalista.

A autora acabou por atribuir a designação *structural power* (poder estrutural) ao balanço de poderes entre Estado e setor privado. O poder estrutural de que fala, comporta quatro grandes áreas: segurança; finanças; produção e conhecimento. Estas áreas foram alvo de análise e a autora acabou por relacioná-las entre si, de tal forma que o seu objetivo passou por perceber quem detém poder num dado período, os motivos que levaram a alterações de detentores de poder em diferentes períodos e quais as consequências dessas alterações. Assim, em todo o seu trabalho, Susan Strange integra uma questão principal na análise do poder, na sua associação entre as

¹³ Tradução livre de: (...) the essence of realism as I understand it is the acknowledgement that outcomes, even in matters of trade and finance cannot be properly analysed (...) in disregard of the distribution of power.

vertentes do poder político e do poder económico. Essa questão é: “*Cui bono?*”. Ou seja, “Quem vai beneficiar do poder estrutural?”. Com esta questão, Strange tenta compreender as relações existentes entre o Estado e as empresas no que à política e à economia diz respeito. Considera que o poder pode ter a participação de outras entidades, além do Estado, ou seja pode haver diferentes detentores de poder. É devido a esta nova abordagem que passa a identificar-se como “*a new realist*” (uma nova realista).

A autora levantou a hipótese de que novas entidades – empresas privadas – passaram a deter um poder determinante na cena internacional. O setor privado, e a importância crescente deste ao nível global, determina hoje, em grande medida as interações entre si e os Estados e, ainda, as interações entre as instituições internacionais e os Estados. Esta hipótese levantada foi uma consequência do fenómeno da globalização, que permitiu que novos mercados mundiais se formassem. Por outro lado, a hipótese já referida levou a que os Estados, até hoje, requeressem a sua própria participação assídua nestes novos mercados, com o objetivo da sua sobrevivência. Exemplos desta participação e interação com o setor privado são as medidas tomadas para atrair investimento para o país e atrair empresas transnacionais a alocarem-se no seu território, como a privatização, a desregulamentação e a liberalização dos mercados. Assim, o Estado procedeu a mudanças relativamente à importância da posição e papel das empresas para as decisões políticas, acabando por lhes ceder alguma autonomia. As palavras da autora são ilustrativas destas ideias:

“Isso parece-me ser um recuo perante o poder dos mercados e dos operadores financeiros. E se alguma vez existiu uma descrição do poder estrutural das crenças e ideias na economia política, é certamente esta. Não foi o poder dos EUA ou do FMI que persuadiu a França ou a Alemanha a privatizar, desregulamentar e liberalizar os seus mercados financeiros. Foi a mudança estrutural na economia de mercado mundial, o imperativo da concorrência pelas quotas de mercado e a mudança subjacente na estrutura do conhecimento, refletida então no poder da estrutura financeira.” (Strange 1998, 9)¹⁴.

O valor acrescentado pelo mercado transnacional levou os Estados a competirem entre si para atrair as melhores empresas, aquelas que são portadoras de uma ação significativa sobre os

¹⁴ Tradução livre de: That seems to me to be a retreat before the power of markets and financial operators. And if ever there was a description of the structural power of beliefs and ideas in political economy, this is surely it. It was not the power of the US or the IMF that persuaded France or Germany to privatise, to deregulate and to liberalise their financial markets. It was structural change in the world market economy, the imperative of competition for market shares and underlying change in the knowledge structure, reflected then in the power of the financial structure.

mercados. Como consequência desta competição passou a existir negociação premente entre governos e empresas que, na maioria das vezes, levou a que fossem facultadas a estas, diversas mais-valias, tais como incentivos ao lucro e o renunciar à aplicação de certas normas e privações. Sempre com vista ao objetivo maior: ser a escolha das empresas estrangeiras para se acomodarem no país. Este argumento levou, mais uma vez, a autora a refletir sobre os efeitos erosivos na autoridade do Estado, relativamente à diminuição do poder em termos de tributação das empresas e de regulamentação dos próprios mercados. (Strange 1995, 60).

Susan Strange analisou vários aspetos da interação existente entre Estado e setor privado, tendo verificado que todos influenciam a dinâmica de poder e consequentemente são aspetos que se relacionam com o tema central desta dissertação. Serão abordados de seguida esses aspetos da relação de poder entre Estado e setor privado.

As quatro estruturas incorporadas pela autora na análise do poder estrutural constroem uma nova faceta do poder, aplicada à política internacional. A saber, passa a existir exercício político por parte dos intervenientes da economia, ou seja, as empresas (transnacionais prestadoras de serviços, tecnológicas, de capital e outras) passam a exercer política, o que culminou na noção de perda de autoridade por parte do Estado. Ainda assim, Strange fez ressalvas no que diz respeito a esta perda de autoridade. No seu entendimento, a globalização é real e esta perda de autoridade também o é, no entanto, o poder do Estado não deixou de se verificar, ou seja, a perda não foi total. O Estado determina até onde vai a globalização quanto às suas políticas internas e externas. Passou, então, a existir divisão de poderes entre o Estado e as outras entidades. Acrescente-se ainda que, mesmo com esta partilha de autoridade, é de salientar que os EUA continuam a defender a sua hegemonia.

Outro ponto relevante para esta dissertação, verificado na análise do estado da arte, é o complexo militar-industrial, sobre o qual Susan Strange também se debruçou. Apesar de Strange ter refletido, já em 1995 (e registado as suas reflexões na obra "*The Defective State*") sobre este complexo, observa-se que ainda hoje ele se verifica. O complexo militar-industrial serve para mostrar que, embora os Estados estejam conscientes dos custos e das repercussões de iniciar uma guerra, continuam a investir na manutenção e desenvolvimento das suas capacidades militares e de defesa. Este complexo militar-industrial resultou do apoio e recurso dos governos a empresas de defesa, através de contratos mantidos entre os dois, que posterior e consequentemente levou ao ganho de quotas de mercado. As empresas associadas à defesa demonstram o desenvolvimento da tecnologia, no qual o Estado se irá suportar (Strange 1995,

62). Esta preocupação dos Estados, que Strange assumiu há cerca de três décadas, veio a verificar-se útil, sendo o exemplo mais atual a guerra na Ucrânia. Não se inclui nestas ideias de evolução da defesa apenas os EUA, mas também a Rússia, a Coreia do Norte e outros países.

Esta dinâmica verifica-se, do ponto de vista realista, pela existência, sempre presente, de ameaça de guerra. Strange reforça, com estes argumentos, a sua ideia de “novo realismo”, pelo facto de o Estado desenvolver a sua capacidade militar através do conhecimento e ajuda das empresas. É, então, possível observar aqui, as áreas “segurança” e “conhecimento” do poder estrutural de Strange relacionadas.

No que diz respeito às áreas “finanças” e “produção”, também é possível observar a sua existência a partir das mudanças provocadas a nível global no poder. As empresas transnacionais passaram a estar por trás do sistema financeiro ligado às suas atividades. A produção recaiu sobre si mesmas também. O poder associado a estas duas áreas reverteu para as empresas. Para além das empresas terem a responsabilização pela localização das suas atividades de produção, assumem também responsabilidades jurídicas e relacionadas com o bem-estar da comunidade onde estão inseridas. As empresas assumem novas funções políticas que caracterizam o sistema internacional onde está inserida uma economia capitalista, funções essas antes assumidas pelo Estado.

“As empresas, respondendo aos mercados, efetuam mais mudanças em menos tempo na distribuição da riqueza na economia global do que todas as organizações internacionais e programas de ajuda bilateral fizeram em quase meio século. As empresas estão também (...) a assumir um papel político muito maior na prestação de assistência social.” (Strange 1995, 69)¹⁵.

Assim, as empresas passaram a ser os novos atores na política e na economia internacional, pois passaram a dar resposta às falhas e inseguranças do Estado, relativamente às novas necessidades da sociedade dos séculos XX e XXI. Foram as empresas que passaram a garantir o processo de inovação devido ao seu poder sobre os campos financeiro e económico, pois eram elas que detinham o nível de conhecimento e competência necessário, neste âmbito. (Strange 1998, 14).

¹⁵ Tradução livre: Firms, responding to markets, effect more change in less time in the distribution of wealth in the global economy than all the international organizations and bilateral aid programs have done in nearly half a century. Firms are also (...) assuming a much greater political role in the provision of welfare.

A relação de poderes estabelecida entre Estado e setor privado passou a ser determinada pela nova diplomacia existente entre estes atores das Relações Internacionais. Esta diplomacia passou a ser estabelecida pelo exercício de poder de negociação das empresas e pela cobiça dos Estados pelos ativos derivados das mesmas, tais como os, já referidos, acesso aos mercados mundiais e acesso à tecnologia avançada (Strange 1995, 68).

É de notar que, a hipótese de que o setor privado detém um poder igual ao dos Estados, ou que o mesmo é transferível de uma unidade para a outra é afastada por Susan Strange. Desta forma, verificou-se uma assunção de que agora o Estado assume um poder estrutural partilhado com as empresas sendo que perde, ao mesmo tempo, parte da sua autoridade e legitimidade em questões ligadas à atividade destas mesmas empresas. Nesta premissa, verifica-se uma nova forma de encarar o papel do Estado no sistema internacional e, o próprio papel das novas empresas transnacionais nos domínios referidos anteriormente. Como consequência desta partilha de áreas de poder entre Estado e setor privado, Susan Strange cria um novo conceito associado à nova condição do Estado. Chama-lhe *Defective State* (Estado com defeitos). O Estado não tem possibilidades de dar respostas rápidas e eficazes a todas as necessidades da sociedade e por isso terá que realizar trabalho conjunto com as empresas dos diferentes ramos já referidos, exercendo, estas, por sua vez, ação política sobre os governos e a sociedade:

“Quando a empresa tem muitos intervenientes políticos em vez de um, e quando sente que tem de parecer um "bom cidadão" aos Estados anfitriões que não o seu Estado de origem, encontra-se envolvida num malabarismo político, ao negociar com ministérios, organizadores do trabalho, fornecedores e distribuidores em vários países ao mesmo tempo. Os governos, por seu lado, tornaram-se extremamente conscientes de que estão a competir como pretendentes rivais, pelos favores das empresas estrangeiras.” (Strange 1995, 59)¹⁶.

Apesar de a reflexão de Susan Strange não ser uma reflexão recente, a análise sobre o poder e a sua correlação com a posição do Estado é uma questão importante e que se enquadra no tema de investigação aqui presente. A autora colocou em perspetiva a hipótese de novas entidades deterem um poder determinante na cena internacional, que até então pertenceria

¹⁶ Tradução livre de: Once the firm has many political masters instead of one, and once it senses that it has to appear a "good citizen" of host states other than its state of origin, it becomes engaged in a political juggling act, negotiating with ministries, labor organizers, and suppliers and distributors in several countries at once. Governments, for their part, have become acutely aware that they are competing, as rival suitors, for the favors of foreign firms.

apenas ao Estado. A autora refletiu sobre a pertinência do papel das novas empresas transnacionais, concluindo que, sendo o poder atribuído a uma entidade que não o Estado, é necessário acautelar certas, determinadas e já referidas situações.

Por fim, e para concluir a revisão da bibliografia, é necessário afirmar que, na mesma, é notória a investigação sobre questões de privacidade, de *BigData* e de soberania digital. Verifica-se uma consciencialização da importância das temáticas “privacidade” e “dados pessoais”, devida ao crescente questionamento sobre a participação da sociedade nas decisões referentes à prática lucrativa da utilização de dados pessoais.

Os direitos sobre os dados dos indivíduos estão constantemente inseridos no jogo económico das grandes empresas, a cada clique realizado e, estão incluídos nas decisões económicas e políticas daqueles que tentam fazer o balanço de poder, os Estados e as empresas privadas. Percebe-se, também, na análise da revisão da bibliografia que há um crescente envolvimento das empresas na definição e formulação de políticas e uma crescente necessidade de os Estados convocarem as empresas para discutir segurança, prosperidade e sobrevivência.

3. Perspetiva Metodológica

3.1. Epistemologia e Ontologia

A presente dissertação baseia-se numa abordagem analítica, a do Capitalismo de Vigilância. O objetivo desta dissertação não é a construção de uma teoria geral, mas sim a compreensão e classificação de partes da realidade, tal como diferenciam Marsh e Furlong (Marsh e Furlong 2018).

É relevante refletir sobre a posição epistemológica¹⁷ e a posição ontológica¹⁸ adotadas nesta dissertação. É importante ter em conta que os vários métodos de análise da investigação levam a que os investigadores em Relações Internacionais se posicionem de forma diferente (Marsh e Furlong 2018).

Relativamente à epistemologia, é possível enquadrar a atual investigação no realismo, referido por Marsh e Furlong (2018), uma vez que este posicionamento epistemológico combina

¹⁷ A epistemologia pretende refletir sobre aquilo que podemos conhecer acerca do mundo (Marsh e Furlong 2018).

¹⁸ A ontologia está focada na natureza do “ser”, com o questionamento sobre a possibilidade de uma realidade independente do nosso conhecimento (Marsh e Furlong 2018).

aspectos do positivismo e do interpretativismo, como o identificar e o analisar a realidade externa observável e o ter em conta a construção social do que é essa realidade, de forma a interpretar as ligações entre fenómenos sociais, respetivamente.

Relativamente à ontologia, é possível enquadrar a investigação no grupo de fundacionalistas porque, parte da realidade associada aos assuntos analisados é observável. No entanto, este enquadramento no grupo dos fundacionalistas, é afastado do positivismo por se entender que existem certos fenómenos sociais e relações entre estes que não são observáveis e que há ainda estruturas embebidas nestes fenómenos que não são, também elas, diretamente observáveis. Assim, admitindo que fenómenos sociais existem independentemente da nossa interpretação dos mesmos, essa interpretação pode, porém, afetar os resultados da ‘realidade’ socialmente construída (Marsh e Furlong 2018).

Nesta dissertação, reconhece-se que existe um espaço digital onde há uma troca produtiva entre utilizadores e não-utilizadores, ou seja, há uma realidade observável enquadrada no entendimento dos fundacionalistas. Mas, como se deu lugar a que a orientação económica dos capitalistas de vigilância determinasse a rota do ciberespaço pelo seu entendimento de como deve ser a realidade digital, esta dissertação pode ser enquadrada no realismo pela sua vertente interpretativista da lógica capitalista.

3.2. O estudo de caso

Para esta dissertação foi escolhida uma abordagem de estudo de caso, sendo que, a problemática da cooperação entre os EUA e a empresa *Palantir Technologies*, no que diz respeito à vigilância em massa de dados, comporta esse mesmo estudo de caso para esta dissertação. Coloca-se ainda, em destaque, a conduta desorientada da respetiva empresa. Esta escolha reflete o interesse pela temática aqui abordada, uma vez que, esta empresa desde a sua criação apresenta uma ligação próxima às unidades de segurança e agências governamentais dos EUA¹⁹, ligação analisada no terceiro capítulo desta dissertação. No entanto, é também uma escolha

¹⁹ Lista de contratos de *Palantir Technologies* com agências governamentais, pelo Federal *Procurement Data System*, um repositório de consulta de milhões de ações contratuais federais: <https://www.fpds.gov/ezsearch/search.do?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir&renderer=isp&length=1274>; Lista de contratos mais recentes, 2022-2023: <https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir+2023&renderer=isp&length=130>

pertinente pelos motivos já referidos na revisão da bibliografia ao integrar a análise de um caso em particular de aplicação²⁰ da abordagem teórica do capitalismo de vigilância.

De notar que, apesar dos EUA não serem aqui classificados enquanto estudo de caso, é importante dizer que o país é central na análise desta investigação. Isto porque, a sede da empresa *Palantir Technologies* é nos EUA e também, como já foi referido, é investigada nesta dissertação, de forma aprofundada, a relação próxima entre Estado e setor privado na utilização lucrativa dos dados dos cidadãos. Assim sendo, os EUA são a escolha preferencial para esta análise devido ao repertório de contratos estabelecidos com a empresa *Palantir Technologies*, que vem demonstrar a importância do estudo da cooperação entre agências governamentais, Departamentos da Polícia norte-americana e a empresa *Palantir Technologies*, devido às implicações que têm no quotidiano dos utilizadores do domínio do digital do século XXI.

3.3. Tipo de estudo de caso

Com base na bibliografia, é possível determinar a tipologia do estudo de caso aqui presente que, de acordo com Jack S. Levy (2008, 6-7), representa um *illustrative case study* (estudo de caso ilustrativo). O objetivo da utilização deste tipo de estudo de caso é dar ao leitor uma orientação quanto ao argumento teórico proposto na investigação, através da exemplificação concreta da aplicação do mesmo ou, de forma a mostrar a relevância empírica de uma proposição teórica é identificado pelo menos um caso relevante de aplicação. Este tipo de estudo de caso enquadra-se no plano maior de *plausibility probe*, que é equiparado a um estudo-piloto numa investigação experimental, na medida em que, pretende explorar a sustentabilidade de um caso particular como veículo para testar uma teoria (Levy 2008,6).

Assim, com esta dissertação pretende-se transmitir a validade do argumento presente na abordagem analítica utilizada, a do Capitalismo de Vigilância, com a análise da dinâmica presente entre Estado e setor privado na utilização lucrativa dos dados pessoais da população. Com a exemplificação de um estudo de caso em particular, *Palantir Technologies*, conseguimos entender os métodos pelos quais a colaboração próxima entre esta empresa e agências governamentais norte-americanas opera no quadro de segurança da população, bem como na colaboração com

²⁰ Importa mencionar que para assegurar a abrangência do estudo de caso optou-se pela análise da cooperação entre *Palantir Technologies* e unidades de segurança regionais, como os Departamentos da Polícia de Los Angeles e de Nova Orleães, bem como na análise da cooperação com uma divisão do nível federal, com análise da parceria de *Palantir Technologies* com uma divisão do Departamento de Segurança Interna dos EUA, a agência *ICE*. Pelo facto desta dissertação não se limitar a um Departamento da Polícia em particular e a uma agência governamental em particular, introduz à investigação uma complexidade acrescida.

Departamentos da Polícia, *ICE*, Departamento da Polícia de *Los Angeles* e o Departamento da Polícia de Nova Orleães, respetivamente.

Com base na bibliografia e tendo em conta os parâmetros estabelecidos por Jack S. Levy (2008, 6-7), é possível identificar este estudo de caso como sendo um estudo de caso ilustrativo. Segundo este autor, a utilização deste tipo de estudo de caso pode ter dois objetivos: dar ao leitor uma orientação quanto ao argumento teórico proposto na investigação, através da exemplificação concreta da aplicação do mesmo ou mostrar a relevância empírica de uma proposição teórica através da identificação de pelo menos um caso relevante de aplicação. Este tipo de estudo de caso enquadra-se no plano maior de *plausibility probe* (investigação da plausibilidade), que é equiparado a um estudo-piloto numa investigação experimental, na medida em que, pretende explorar a sustentabilidade de um caso particular como veículo para testar uma teoria (Levy 2008,6).

Assim, o estudo de caso abordado nesta dissertação é considerado um estudo de caso ilustrativo pois atinge os dois objetivos referidos. Por um lado, pretende-se transmitir a validade do argumento presente na abordagem analítica utilizada, a do capitalismo de vigilância, com a exemplificação de um estudo de caso em particular, a empresa *Palantir Technologies* e a sua cooperação com unidades de segurança dos EUA. E, por outro lado, este mesmo estudo de caso mostra a relevância empírica do capitalismo de vigilância, que ainda é apenas uma proposição teórica.

4. Métodos e Recolha de dados

Esta dissertação baseia-se na investigação sobre a forma como se desenrola a cooperação entre o Estado e o setor privado, na vigilância de dados e, para isso, recorreu-se a fontes primárias (exemplos: documentos oficiais dos Departamentos da Polícia de Los Angeles e Nova Orleães, e da divisão governamental ICE; relatórios de avaliação do impacto das colaborações entre a empresa *Palantir Technologies* e as entidades referidas; apresentações internas acerca da missão conjunta entre estes atores, produzidas pela empresa *Palantir Technologies*; documentos oficiais de iniciativas federais tais como, *Homeland Security Act* criada pelo Departamento de Segurança Interna dos EUA e a *Smart Policing Initiative* pelo Departamento de Justiça dos EUA) e a bibliografia secundária (exemplos: artigos científicos; livros e capítulos de livros). Para além destas fontes, contou-se ainda com outra mais-valia – uma entrevista semiestruturada a um representante da empresa *Palantir Technologies*, realizada no dia 24 de maio de 2023, que contribuiu para a obtenção de informações cruciais para a dissertação. Os contributos desta entrevista foram

incorporados no desenvolvimento da mesma. A entrevista foi importante pois permitiu obter informações, opiniões e clarividades nessa área, o que facilitou a análise do estudo de caso.

Nesta altura, torna-se necessário realizar uma ressalva relativamente ao estudo de caso escolhido: as fontes selecionadas e apresentadas nesta dissertação não foram escolhidas por corroborarem a hipótese sugerida nesta investigação, mas antes por estarem disponíveis de forma mais acessível e por conterem informações mais completas.

5. Estrutura da dissertação

O primeiro capítulo desta dissertação refere-se à abordagem teórica do Capitalismo de Vigilância, onde se analisa os seus primeiros sinais, no século XXI, bem como as suas principais características e imperativos de ação, perante o domínio do digital. Neste capítulo, são salientados aspetos e estratégias cruciais para o desenvolvimento do Capitalismo de Vigilância. Alguns desses aspetos são o contexto histórico em que se insere, que permitiu que fossem desenvolvidas e criadas “afinidades eletivas” entre o Estado e o setor privado; o sistema neoliberal característico dos EUA que restringe e não procura a regulamentação destas empresas, criando uma dificuldade na garantia da proteção e privacidade dos dados da população e; o desenvolvimento de uma nova forma de poder, que permite certificar às empresas a garantia do contínuo acesso aos dados.

O segundo capítulo desta dissertação corresponde à análise da mudança da perceção dos EUA perante o papel das suas unidades e agências de segurança, desde as unidades da Comunidade de Inteligência até às unidades mais pequenas, responsáveis pela garantia da segurança pública no terreno, os Departamentos da Polícia. Os EUA tiveram de redirecionar as suas atenções para as suas políticas internas, no imediato ao 11 de setembro, de forma a devolver a segurança nacional sucumbida ao terrorismo transnacional. Este contexto de emergência securitária permitiu a elaboração e introdução de iniciativas que expandiram a ação dos departamentos no combate ao terrorismo e, expandiram a comunicação entre fontes de dados institucionais pelos Estados, a saber: o *Homeland Security Act* de 2002 e a *Smart Policing Initiative* de 2009, respetivamente. Através destas iniciativas, foram atribuídos fundos às unidades de segurança de modo a que estas se desenvolvessem e adotassem estratégias orientadas por dados, o que permitiria uma melhor resposta das mesmas às exigências securitárias associadas à tecnologia do século XXI. Neste caso em particular, as estratégias orientadas por dados, referem-se à recolha de informação sobre a população e sobre as suas interações. Assim, surge o conceito de *intelligence-led policing*, que consiste num novo policiamento associado à recolha de

informações, acentuado pelos novos métodos analíticos e preditivos oferecidos pelas empresas privadas.

O terceiro e último capítulo desta dissertação refere-se à exploração da arquitetura do Capitalismo de Vigilância aplicada ao estudo de caso, a cooperação entre os EUA e a empresa *Palantir Technologies*. Aqui, são dissecadas as interações entre Estado e setor privado, mais especificamente entre os Departamentos da Polícia e as agências governamentais norte-americanas e a empresa *Palantir Technologies*, por ordem cronológica das parcerias. Neste capítulo, o foco está na cooperação, a um nível mais exíguo, entre o Departamento da Polícia de Los Angeles e a empresa *Palantir Technologies*, entre o Departamento da Polícia de Nova Orleães e a empresa *Palantir Technologies* e, ao nível federal, entre a agência governamental ICE e a empresa *Palantir Technologies*.

Neste mesmo capítulo são analisadas as tarefas, os papéis e as estratégias usadas pela empresa na utilização dos dados da população provenientes de fontes institucionais e não institucionais. As tarefas, os papéis e as estratégias são usadas de forma a responder a momentos de crise na atuação dos Departamentos da Polícia com vista à garantia da segurança pública e, protegidas pelas diretivas securitárias. Na análise de documentos associados à contratação da empresa *Palantir Technologies*, para responder às necessidades do Estado, verificou-se que a dinâmica de cooperação entre ambos não atravessava o escrutínio da população, ou seja, os dados que eram utilizados e a forma como eram utilizados não eram do conhecimento da mesma. Esta dinâmica silenciosa colocou em causa a garantia da privacidade da população pelo facto de haver uma contratação e cooperação sigilosa e invisível, aquando da utilização dos dados para garantir resultados a estas entidades.

A conclusão desta dissertação demonstra que a cooperação entre o Estado e o setor privado, em matéria de vigilância de dados, é acentuada pela urgência securitária do pós-11 de setembro e, veio trazer uma necessidade inconvertível de uma lógica de capitalização de informação por parte do Estado sobre a população. Isto é, tendo em conta as vantagens de uma cooperação com as empresas privadas tecnológicas e com o desenvolvimento das suas capacidades analíticas preditivas, o Estado procurou, tal como elas, a vigilância sobre a sua população porque ao ser possível fazer um cálculo e uma gestão do risco dos cidadãos e das suas atividades, obtinha um maior controlo sobre o quotidiano dos mesmos. A combinação entre a urgência securitária e a descoberta de um excedente comportamental libertado pelas pessoas no

domínio do digital, culminou no aparecimento e enraizamento de uma nova lógica de acumulação, o Capitalismo de Vigilância, favorecido pela cooperação permanente entre o Estado e as empresas.

Capítulo I. Abordagem teórica: o capitalismo de vigilância

1.1. Tecnologias de segurança e o ‘complexo industrial de segurança’

Antes de dar início à exploração da abordagem teórica do capitalismo de vigilância no subcapítulo seguinte, será pertinente fazer uma pequena análise sobre o tema das tecnologias de segurança e sobre o ‘complexo industrial de segurança’. Temas que pertencem aos campos interdisciplinares: Estudos de Segurança e Relações Internacionais.

A referência e análise do tema, tecnologias de segurança, é relevante para a dissertação uma vez que, trata-se de uma evolução nas tecnologias de segurança por força da inovação tecnológica, e da necessidade de uma aproximação entre o Estado e o setor privado, o que possibilita, por sua vez, uma maior aproximação às possíveis respostas à pergunta de investigação da dissertação.

Assim, é possível abordar algumas narrativas dentro destes campos de estudo sobre o papel e o impacto da tecnologia em práticas de segurança. Para esta dissertação serve de exemplo de estudo a análise feita no livro de J. Peter Burgess sobre as tecnologias de segurança (2010).

Na obra editada por J. Peter Burgess, é sugerida a divisão da análise em três partes: exploração de abordagens críticas à segurança; exploração da história e sociologia da tecnologia e as suas implicações no século XXI e; exploração das transformações no *doxa* contemporâneo da segurança, bem como nos sistemas tecnológicos atuais que levam à interpretação do desenvolvimento de um ‘complexo industrial de segurança’. A noção de um ‘complexo industrial de segurança’ enquadra a relação entre o governo, as agências de segurança, interna e externa, e a indústria de defesa e o setor das tecnologias de informação. O objetivo da análise passa por compreender melhor a relação contemporânea entre segurança e tecnologia (Burgess 2010).

O ponto crucial destacado na análise do autor é o crescente papel do setor tecnológico (industrial e comercial) nas práticas de segurança, analisado seguidamente.

A tecnologia é entendida como uma componente das práticas de segurança, e não um instrumento ou resultado das mesmas. Destaca-se a centralidade do tema das novas tecnologias

na condução das atividades de segurança externa e interna, quando se analisa a evolução da perspectiva acerca de ameaças e riscos à segurança (Burgess 2010).

Por um lado, existe a narrativa da ordem pós-bipolar do sistema internacional acerca de novas ameaças e riscos à segurança. Ou seja, uma vez que o ‘inimigo’ da Guerra Fria desapareceu, novos desafios surgiram: o sentimento de imprevisibilidade, ressurgimento de ‘conflitos congelados’ e Estados falhados, e a proliferação de armas de destruição maciça. Por outro lado, as narrativas de ‘(in)segurança global’ destacam o estado de globalização do mundo e a difusão de regimes liberais, isto é, regimes à partida predispostos a uma maior abertura de mercado e fronteiras e, por isso, associa-se aos mesmos um risco maior a variáveis transnacionais imprevisíveis (Burgess 2010).

A narrativa de ‘(in)segurança global’ foi acelerada dado os ataques terroristas de 11 de setembro de 2001, e os subsequentes atentados em 2004 e 2005, em Madrid e Londres respetivamente. Com o crescimento do sentimento de insegurança e vulnerabilidade, o objetivo das agências de segurança dos países não é apenas proteger um território e a população, mas também e com maior peso, reduzir a vulnerabilidade, ao antecipar eventos potencialmente ameaçadores. Dado isto, parte do foco dos Estudos de Segurança passa por analisar a mudança progressiva na legitimação, significado e práticas de segurança de uma abordagem de proteção para uma abordagem de gestão do risco. Nesse sentido, existe uma dependência da noção de risco, do cálculo e gestão do risco, que tem sido identificada como um dos principais fatores impulsionadores da inovação nas práticas de segurança, tanto no campo policial como no militar. No cálculo do risco, a tecnologia desempenha um papel crucial para essa transição (Burgess 2010).

Apesar de críticas à consequente dependência tecnológica das agências de segurança dos EUA (país de destaque no contexto das duas narrativas mencionadas), que utilizam métodos de recolha de *intelligence* para um cálculo e gestão do risco mais eficaz, ao invés do recurso exclusivo à capacidade humana, o Departamento de Segurança Interna (*DHS*), criado em 2002, concentrou-se fortemente em atividades e desenvolvimentos tecnológicos. Além disso, o período que se seguiu aos ataques terroristas de 11 de setembro foi marcado pela implementação de programas e medidas de contenção de práticas terroristas, como por exemplo o programa “*Total Information Awareness*”²¹ (2002), renomeado em 2003 para “*Terrorism Information Awareness*” que, em

²¹ Com vista ao alcance de uma capacidade preditiva de novos ataques terroristas, este programa tinha como objetivo integrar e agregar bases de dados de vários organismos públicos e privados (Burgess 2010).

contrapartida levantavam preocupações éticas, sobre privacidade e liberdades civis. Este programa estava em linha com as diretrizes do decreto “*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*”²² (Burgess 2010).

A dependência tecnológica para a recolha de *intelligence* é justificada muitas vezes, com o argumento de que, apesar de falhas residuais, a tecnologia é um pré-requisito obrigatório num contexto de emergência - ‘(in)segurança global. Os sistemas tecnológicos avançados são necessários sobretudo, para permitir que as agências de segurança consigam recolher e partilhar informações através das fronteiras profissionais (por exemplo, polícia local e polícia nacional/federal); setoriais (por exemplo, privado e público); e, nacionais, de forma a solucionar uma série de ameaças. O principal objetivo do uso destes sistemas passa por dominar o incerto e prever o imprevisível (Burgess 2010).

O uso crescente da tecnologia nas práticas de segurança, particularmente o uso da biometria, bases de dados, partilha de informações, extração e exploração de dados servem para a vigilância diária e monitorização de indivíduos e grupos de indivíduos, com a finalidade de antecipar perigos e ameaças. No entanto, como referido, esta vigilância e monitorização levanta questões sobre a segurança coletiva. O uso destas tecnologias para fins militares e de polícia local tem evoluído significativamente ao longo dos anos (Burgess 2010).

A tecnologia, além de envolver a materialidade dos artefactos, abrange formas específicas de fazer e saber, como montar, desmontar, reparar e inventar dispositivos, sendo assim concebida como uma prática. A noção de tecnologia enquanto prática é adotada por alguns autores da história e sociologia da tecnologia, incluindo no livro editado pelo autor já referido, de forma a afastarem-se do argumento tridimensional de inércia tecnológica, irreversibilidade e autonomia. Pelo contrário, a prática da tecnologia deve ser encarada como um processo político-social em constante mudança, mesmo que com algumas consolidações ao longo do tempo. No entanto, a consolidação de certos desenvolvimentos tecnológicos não deve ser tratada como um resultado da inevitabilidade tecnológica, mas antes pelo agregar de um conjunto de dinâmicas complexas e evolutivas de poder entre o coletivo humano (Burgess 2010).

²²Decreto introduzido pouco tempo após os ataques terroristas de 11 de setembro de 2001, sem espaço para debate ou oposição. O decreto permitia às forças de segurança dos EUA alargar a sua vigilância ao: expandir as escutas telefónicas e a monitorização dos registos de chamadas, a nível doméstico e internacional; expandir a autoridade para aceder a comunicações eletrónicas; permitir buscas secretas; remover proteções de privacidade de forma a que as agências de segurança partilhassem informações entre as mesmas; e, ainda, expandir o financiamento às forças de segurança (Electronic Privacy Information Center s.d.)

A tecnologia enquanto prática não é nem revolucionária nem evolutiva nas suas operações, nem segue um processo linear de progresso técnico. Ao invés, os desenvolvimentos tecnológicos são constantemente remodelados em resultado de uma negociação entre os níveis local e geral, social e técnico. Isto é, o desenvolvimento de um sistema tecnológico específico passa por um processo de mediação e negociação que reflete as preocupações, formas de agir e agendas de vários intervenientes, tendo ainda em consideração, tendências e necessidades da sociedade num dado momento (Burgess 2010).

Na abordagem do livro, sobre tecnologias de segurança, é questionada a ingenuidade atribuída à tecnologia. Assim, se a tecnologia constitui um conjunto de processos sociais e práticas sociais, não pode ser considerada alienada dos contextos sociopolítico e económico, concluindo que os desenvolvimentos tecnológicos ‘têm política’ (Burgess 2010).

Nas pesquisas mais recentes dentro dos Estudos de Segurança, a tecnologia é destacada pela sua influência crucial na formulação e condução de políticas de segurança. O ajuste e regulação dos domínios de insegurança depende cada vez mais de processos tecnológicos e tecnocráticos. Ou seja, os desenvolvimentos tecnológicos não são uma resposta direta a uma decisão política, mas frequentemente já existem e estão em funcionamento de alguma forma em certas rotinas profissionais e tecnologias institucionais.

Ao analisar as aplicações de tecnologia nas práticas de segurança contemporânea, o autor conclui que a tecnologia não é apenas uma ferramenta de política ou o resultado direto de uma decisão política, em termos de segurança. A segurança e a tecnologia são práticas inter-relacionadas, isto é, as práticas de segurança desempenham um papel importante na formulação, no desenvolvimento e na promoção de sistemas tecnológicos e, em troca, a tecnologia molda, forma e direciona as práticas de segurança (Burgess 2010).

1.1.1. ‘Complexo industrial de segurança’

Na sequência da abordagem de um contexto de (in)segurança global e de uma necessidade de calcular e colmatar riscos à segurança nacional inferiu-se uma dependência tecnológica das agências de segurança. Uma dependência do setor das tecnologias de informação e de grandes multinacionais, uma vez que permitem a recolha e processamento de informação necessária para o cálculo de risco de novos ataques terroristas ao território nacional.

Esta dinâmica contemporânea entre segurança e tecnologia levou ao surgimento da noção de um ‘complexo industrial de segurança’. O surgimento deste ‘complexo industrial de segurança’

parte de três dinâmicas centrais: a primeira dinâmica sendo o investimento do Estado nas suas forças de segurança por meio de equipamento militar, garantido às empresas de armamento uma fonte de rendimentos crescente, além disso, as fronteiras entre segurança interna e externa, e entre operações militares e da polícia diluíram dada a globalização e transnacionalização de ameaças contemporâneas; a segunda dinâmica passa pela junção do setor das tecnologias de informação às práticas de segurança uma vez que, os desenvolvimentos tecnológicos trazidos pelas grandes empresas permitem às forças de segurança a possibilidade de uma vigilância alargada, da esfera pública e privada, de comunicações, e de indivíduos e grupos de indivíduos; a terceira dinâmica levou à aceleração das duas anteriores, considerando que os investimentos e desenvolvimentos tecnológicos das forças de segurança foram uma tendência e o resultado de uma resposta governamental que se registou, em grande escala, após o 11 de setembro de 2001 com a declaração da 'Guerra ao Terror' (Burgess 2010).

A noção de um 'complexo industrial de segurança' indica que as transformações tecnológicas nas práticas de segurança foram significativas: numa primeira dimensão, estas transformações abrangem a sobreposição das atividades de segurança interna e externa, sobreposição que gera novas exigências tecnológicas para os profissionais de segurança; numa segunda dimensão, e em consequência da primeira, há uma transformação na competitividade dos profissionais das forças de segurança pela especialização e acumulação de conhecimento técnico e prático, que é possível através da reformulação de práticas organizacionais (isto é, com a integração de novos participantes, como por exemplo as empresas tecnológicas no 'complexo industrial de segurança', com mudanças nas atividades de organizações já estabelecidas, no caso das empresas de armamento, e com a formação de novas conexões e parcerias com o setor público); numa terceira e última dimensão, a constituição de um 'complexo industrial de segurança' está também ligada à declaração de uma 'Guerra ao Terror', abordagem que gerou novas perspectivas e exigências tecnológicas para as forças de segurança (Burgess 2010).

A análise das transformações nas práticas organizacionais ao nível das forças de segurança permite refletir sobre as mudanças fundamentais nas estratégias e abordagens adotadas pelas mesmas, e sobre as colaborações com outros setores, nomeadamente o setor tecnológico, de modo que o Estado consiga responder às novas exigências e desafios emergentes que se apresentam.

À luz da integração de 'tecnologias de segurança' e da combinação de dinâmicas entre vários setores no apoio à segurança do território nacional é gerada uma dependência tecnológica,

na procura pelo cálculo e gestão do risco eficaz pelas forças de segurança. A dependência tecnológica das forças de segurança é analisada pela autora Shoshana Zuboff (2019), ao que a autora sugere na sua abordagem teórica do capitalismo de vigilância - a partir do século XXI assiste-se à constituição e consolidação de uma nova ordem económica.

1.2. Capitalismo de vigilância: uma visão geral

De modo a iniciar este capítulo sobre a abordagem teórica escolhida, o capitalismo de vigilância, é pertinente mencionar que esta foi a primeira e única abordagem que se equacionou para a análise do estudo de caso desta dissertação. Assim se procedeu uma vez que, por um lado, se trata de uma abordagem teórica recente, especificamente predisposta para analisar eventos recentes no espectro da economia digital do século XXI e, por outro lado, é a abordagem teórica que dispõe das ferramentas para responder à pergunta de investigação colocada nesta dissertação.

Apesar da designação de capitalismo de vigilância à dinâmica capitalista atual, por Shoshana Zuboff, o conceito já tinha sido proposto por John Bellamy Foster e Robert W. McChesney, a julho de 2014 na revista *Monthly Review*. Apesar da inconveniência genealógica do conceito, cabe aqui referir que a abordagem do capitalismo de vigilância enquanto análise da dinâmica que paira sobre as relações sociais e trocas económicas do século XXI é explorada em detalhe por Shoshana Zuboff, bem como o poder que se encontra na retaguarda, mas como força garante desta lógica capitalista. Devido ao ensaio detalhado da autora, a sua análise é a escolhida para esta dissertação.

Aquando do estudo desta abordagem teórica, foi construída uma tabela para a melhor organização dos pontos centrais do argumento proposto (ver **Tabela 2**). Nesta fase da dissertação, procede-se, então, à apresentação e exploração da abordagem teórica do capitalismo de vigilância, utilizando a mesma tabela como recurso.

Dessa forma, começa-se por explorar o que é, na sua natureza fundamental, o capitalismo de vigilância, e num momento subsequente, analisa-se os fatores que levaram ao desenvolvimento do mesmo.

O capitalismo de vigilância, seguindo a análise da autora Shoshana Zuboff, representa uma lógica de acumulação que, embora partilhe semelhanças com o capitalismo de produção do século XX, apresenta novas leis de movimento, e mais desenvolvidas. Isto é, para além das características inerentes ao capitalismo de produção, como a produção competitiva, a

maximização do lucro, a elevada produtividade e crescimento, acresce a esta versão recente de capitalismo, novas características e imperativos sui generis: “O meu argumento é que, embora o capitalismo de vigilância não abandone as “leis” capitalistas vigentes, (...), esta dinâmica prévia funciona agora no contexto de uma nova lógica de acumulação que também introduz as suas próprias leis do movimento.” (Zuboff 2019, 85).

A partir dos anos 2002 e 2003, os primeiros sinais do capitalismo de vigilância surgiram, e desse ponto em diante, desenvolveu-se a ordem económica imperativa do século XXI, semelhante à representatividade do capitalismo de produção no século XX. Esta ordem não só transformou e moldou a economia, mas também influenciou a sociedade em geral, bem como as dinâmicas atuais de poder, política e cultura. O capitalismo de vigilância representa, assim, a mais recente e atual ordem económica institucional que resultou de um ciclo de reinvestimento do excedente comportamental gerado pelos utilizadores no domínio digital, através da vigilância do mesmo, gerando uma economia de vigilância dos dados (Zuboff 2019).

O capitalismo de vigilância opera no mundo digital, tornando-se uma força impraticável quando removida desse contexto e privada do suporte da tecnologia. Não obstante, não se pode igualar capitalismo de vigilância à tecnologia, ainda que haja por vezes essa condescendência.

Desde o início, é esclarecido pela autora que, o capitalismo de vigilância não é sinónimo de tecnologia, no entanto, é sinónimo de uma lógica capitalista que incorpora a tecnologia e direciona a sua ação em função dos objetivos de mercado dos que abraçam o capitalismo de vigilância. Assim, a tecnologia e o uso dado à mesma são condições sine qua non para a evolução e continuação da estrutura de mercado que o capitalismo de vigilância compõe. A dimensão digital pode assumir diversas formas, essas formas vão, todavia, depender das lógicas sociais e económicas que a orientam para a ação. As lógicas sociais e económicas do capitalismo de vigilância são o tópico de inquietação para a autora Shoshana Zuboff, uma vez que a própria considera que, o uso da tecnologia como expressão dos objetivos económicos do mercado pode ter implicações e apresentar desafios para temas como a privacidade, democracia e a liberdade individual (Zuboff 2019).

O capitalismo de vigilância não pode, assim, ser reduzido a uma mera manifestação tecnológica, como plataformas ou algoritmos. Contudo, é inviável conceber o capitalismo de vigilância sem os recursos do domínio digital, embora seja possível considerar estas tecnologias e as suas capacidades sem a configuração de mercado que é o capitalismo de vigilância (Zuboff 2019b).

Sobre o que é o capitalismo de vigilância, é possível dizer ainda que representa uma forma de mercado que, embora dependa e sobreviva no meio digital, tem como objetivo principal e fim último conseguir operar e moldar circunstâncias no mundo real para garantir os lucros que derivam da vigilância do digital, mas também cada vez mais da realidade “tangível”. Esta abordagem visa não só a exploração dos dados digitais, mas também procura influenciar e controlar as interações e comportamentos dos indivíduos no mundo físico, tudo isto em prol do aumento dos lucros (Zuboff 2019).

O mercado é representado, nesta dissertação, pelo conjunto de empresas privadas que fazem esta coleção massiva de dados procurando extrair valor monetário dos mesmos, mas que procuram, ao mesmo tempo, prever e influenciar o comportamento humano, alimentando desta forma um ciclo de vigilância e controle sobre informação e dados sem precedentes.

De que forma é que foi possível que o capitalismo de vigilância se desenvolvesse? Que fatores contribuíram para o favorecimento desta lógica de acumulação? São perguntas que vão ser respondidas nos subcapítulos que se seguem.

É pertinente, no entanto, explicar ainda neste subcapítulo que, a origem do capitalismo de vigilância assenta em dois momentos principais, apesar de serem mais bem analisados, também estes, nos subcapítulos seguintes. O primeiro momento prende-se com o período de crise atravessado pela Google em 2001 e, a sua consequente procura expansiva por lucros, que se traduziu na descoberta do valor dos dados e no desenvolvimento de um modelo de negócio que se baseia na coleção e análise desses mesmos dados, considerando aqui a empresa Google como a empresa pioneira deste processo de comoditização dos dados. O segundo momento é o período que se seguiu aos acontecimentos do dia 11 de setembro de 2001, isto é, o estado de guarnição que se instaurou nos EUA em termos securitários e, em termos de aprovação de leis que permitiam uma vigilância mais alargada para uma previsão de eventos semelhantes (Zuboff 2019).

Estes dois momentos, apesar de parecerem independentes um do outro, à primeira observação, estão, no entanto, no que diz respeito à sua contribuição para o desenvolvimento da ordem institucionalizada do capitalismo de vigilância, sincronizados. Isto é, o período de insegurança que o país atravessava juntava-se à procura das empresas privadas pela caixa de pandora do excedente comportamental que a Google tinha desvelado. Estas duas dinâmicas resultaram numa aproximação do Estado às empresas privadas, desenvolvendo-se uma sinergia interdependente entre ambos - ao que a autora intitula de afinidades eletivas (Zuboff 2019).

As forças motrizes do capitalismo de vigilância, como os imperativos de extração e previsão, e também as economias de escala, âmbito e ação são analisadas no subcapítulo que se segue.

1.3. As principais características do capitalismo de vigilância

Como já referido, o capitalismo de vigilância representa uma lógica de acumulação. Uma acumulação de dados e uma acumulação de lucros. A acumulação compõe o motor principal do capitalismo de vigilância, do qual imperativos económicos podem ser deduzidos.

Com a descoberta da Google do excedente comportamental dos utilizadores no digital, isto é, dos dados comportamentais que se podem deduzir de uma pesquisa na internet acerca dos indivíduos, foi possível para a mesma reinventar-se no decurso de uma emergência financeira em Silicon Valley, e de uma pressão dos investidores. Assim, o capitalismo de vigilância surge enquanto solução para uma crise, materializando-se numa metodologia rápida que converteu e converte o investimento em receitas e capital.

Esta descoberta e comoditização de dados comportamentais pela Google foi abraçada por outras empresas, no entanto, esta lógica não pode ser compreendida separada das condições históricas únicas que lhe foram transversais, as quais inicialmente motivaram a procura urgente por uma nova forma de mercado e que, mais tarde, sustentaram e protegeram os mecanismos de acumulação que lhe são inerentes (Zuboff 2019).

O que começou por ser uma troca válida entre utilizadores e prestadores de serviços tornou-se, rapidamente, de um modo implícito, numa atração de excedente comportamental e os utilizadores passaram a ser provedores involuntários de matéria-prima para um ciclo amplo de geração de receitas (Zuboff 2019). Por outras palavras, num período inicial, os dados extraídos do comportamento dos utilizadores no meio digital eram transformados, exclusivamente, em melhorias no sistema da Google que beneficiavam os utilizadores. A exploração dos dados dos utilizadores proporcionava um valor sem custos, sendo este valor reinvestido na experiência dos utilizadores, na forma de serviços aprimorados - melhorias que eram também disponibilizadas aos utilizadores sem custos adicionais (Zuboff 2019)

Os utilizadores funcionam nesta lógica como fonte de matéria-prima: dados comportamentais. No começo, os utilizadores forneciam, então, esta matéria-prima na forma de dados comportamentais, os quais eram posteriormente recolhidos para otimizar a velocidade, precisão e relevância, além de ajudar a desenvolver produtos complementares auxiliares, como a

tradução. Shoshana Zuboff intitula esse processo de ciclo de reinvestimento do valor comportamental, no qual todos os dados comportamentais são reinvestidos na melhoria contínua do produto ou serviço (Zuboff 2019).

Dada a situação excecional de crise que se sentia entre as empresas de Silicon Valley, (tendo em conta o enquadramento do financiamento de risco neste epicentro, em 2001 criaram-se níveis perigosos de valorizações inflacionadas, contribuindo para um sentimento de instabilidade e emergência na empresa Google) medidas extraordinárias foram tomadas pelas mesmas, o credo dessas entidades passou a ser: “(...), quem quiser permanecer na vanguarda não poderá apresentar apenas capacidade para ganhar dinheiro. Será preciso apresentar capacidade para lucros sustentáveis e exponenciais.” (Kara Swisher citada por Zuboff 2019, 92). Ou seja, as medidas extraordinárias traduziam-se em métodos que resultassem em retornos rápidos e num crescente retorno do valor líquido. Esta era a métrica de sucesso em Silicon Valley num contexto de crise: “A declaração do estado de exceção funciona na política como cobertura para a suspensão do estado de direito e para a intrusão de um novo poder executivo justificado pela crise.” (Zuboff 2019, 93).

Os retornos rápidos manifestaram-se através da aposta na publicidade. Ao contrário da posição antagónica anteriormente adotada pelos fundadores, essa postura não se verificou após a crise. O surgimento de anúncios e anunciantes implicou que terceiros passaram a ter presença no espaço digital da Google. Os anúncios apresentados aos utilizadores eram geridos pela empresa, de acordo com a sua análise do excedente de dados comportamentais dos utilizadores. No final da década de 2000, a nova abordagem da empresa justificava-se com a ideia de que os anúncios deveriam ser relevantes para os utilizadores, indo além das palavras-chave da pesquisa para direccionar anúncios específicos a indivíduos. Para alcançar esse objetivo, o ciclo de reinvestimento do valor comportamental foi redireccionado para um projeto mais amplo e complexo (Zuboff 2019).

De forma concisa, a abordagem adotada baseava-se no uso de dados comportamentais, anteriormente utilizados para melhorar a qualidade dos resultados das pesquisas, para direccionar publicidade aos utilizadores individuais. E, embora uma parte desses dados continuasse a ser usada para melhorar o serviço da empresa, uma parte crescente estava a ser direccionada para aprimorar a rentabilidade dos anúncios, tanto para a Google quanto para os anunciantes (Zuboff 2019).

Por outras palavras, a Google tinha conseguido criar o contexto para aplicar práticas fora do comum e avançar com estratégias que permitiam uma acumulação de dados dos utilizadores e a sua comoditização. Estas operações, mais apropriadamente descritas como operações de vigilância, expandiram de forma acelerada e inovadora, sem os impedimentos que existiriam sob normas habituais. Este estado de exceção, proporcionado por uma crise, foi fundamental para o desenvolvimento do capitalismo de vigilância, permitindo à empresa explorar estratégias que iriam permitir uma acumulação maior de uma diversidade de dados, o que por consequência se traduziria na acumulação de lucros.

O estado de exceção que levou à descoberta e compreensão do potencial preditivo dos dados transformou o capitalismo da informação num projeto de vigilância lucrativo. A partir deste ponto, a empresa combinou inteligência artificial sofisticada e a contínua recolha de excedente comportamental, o que se tornaria a base de uma lógica de acumulação de lucros e de dados sem precedentes. Um exemplo prático desse ineditismo é a patente submetida pela Google, em 2003: “gerar informações do utilizador para uso em publicidade direcionada”²³, é um marco que ilustra o uso de dados comportamentais para personalizar anúncios com base nos interesses inferidos dos utilizadores a partir da vigilância dos seus comportamentos online (Google Inc. 2003; Zuboff 2019).

Os cientistas da Google perceberam que a experiência humana podia ser comoditizada, descobriram uma matéria-prima “virgem” que podia ser extraída a custo baixo. O excedente comportamental gerado pelos utilizadores formou a base para uma nova dinâmica de trocas de mercado. Uma nova “ficção mercantil”, isto é, mais um alicerce para uma economia de mercado autorregulada: a sombra digital dos utilizadores. Assim, a experiência humana no mundo digital foi transformada em dados comportamentais, dados inseridos nos mercados de comportamentos futuros e considerados ativos de vigilância. Estas descobertas e transformações na trajetória da Google e das empresas que se seguiram alteraram a trajetória do capitalismo da informação ao consentir a utilização da experiência humana por uma dinâmica de mercado sem impedimentos na internet, onde o conhecimento e o poder passaram a residir no capital de vigilância (Zuboff 2019).

Voltando à pergunta colocada no início deste capítulo, sobre a abordagem teórica: de que forma é que foi possível que o capitalismo de vigilância se desenvolvesse? É possível responder a

²³ Tradução livre de: Generating User Information For Use in Targeted Advertising

esta pergunta explorando, seguidamente, os imperativos categóricos do capitalismo de vigilância, que são as leis do novo mercado vigilante que permitem movimentar os ativos de vigilância.

1.4. Os imperativos que sustentam o capitalismo de vigilância

De forma a manter e a desenvolver esta lógica de acumulação através da vigilância, as empresas compreenderam que era necessária a aposta na previsão para a contínua acumulação de capital. Mas, tal como a publicidade também sempre foi um desafio de previsão, pois trata-se de uma combinação entre arte, relacionamentos, senso comum, mas não se trata de uma ciência exata (Zuboff 2019).

As empresas aprimoraram esta prática preditiva com a contínua evolução do capitalismo de vigilância, no entanto, o objetivo é essencialmente sempre o mesmo: entregar uma mensagem específica a um indivíduo específico, no momento exato em que essa mesma mensagem tenha uma maior probabilidade de influenciar o seu comportamento. Este é o credo da publicidade (Zuboff 2019).

A Google, como pioneira, lançou, para além desta descoberta das vantagens do uso do excedente comportamental dos seus utilizadores, os mecanismos necessários para a acumulação e previsão do mesmo (Zuboff 2019). Assim sendo, apresenta-se agora os imperativos que ditam a contínua institucionalização do capitalismo de vigilância e da ação dos capitalistas de vigilância: o imperativo de extração e as economias de escala; o imperativo da previsão e as economias de âmbito; e, finalmente, o imperativo da previsão e as economias de ação. São também os imperativos que ditaram a ascensão dos lucros provenientes da vigilância, intensificando a competição pelas receitas do mercado de “futuros comportamentais”.

1.4.1. O imperativo de extração e as economias de escala

A eficácia dos produtos de previsão está diretamente relacionada com o volume de dados processados por sistemas automatizados. Assim, a acumulação de grandes volumes de dados torna-se uma exigência competitiva entre as empresas. Este parâmetro apresenta o imperativo de extração de dados do capitalismo de vigilância, um reflexo da necessidade de economias de escala na acumulação de excedente comportamental.

Sendo a acumulação de dados comportamentais, o principal e o motor instrutor do capitalismo de vigilância cabe às empresas tecnológicas assegurar sistemas automatizados que

monitorem, capturem e induzam a produção de mais dados comportamentais apurados pelo comportamento online dos utilizadores.

De notar que as empresas compreenderam que, para realizar previsões mais precisas e obter lucros maiores, a acumulação de dados não poderia estar limitada apenas ao ambiente digital, uma vez que esses mesmos dados comportamentais estavam restritos ao comportamento dos utilizadores online, o que não reflete “toda a realidade” do utilizador. Por conseguinte, os sistemas computacionais são hoje incorporados em produtos e dispositivos de assistência ao utilizador no mundo físico, como assistentes de voz (por exemplo, Alexa da Amazon; Cortana da Microsoft); aspiradores autónomos que mapeiam a casa; e, sistemas de alarme com tecnologia biométrica. Estes sistemas, preparados para acumular excedente comportamental na “realidade tangível”, formam uma arquitetura de extração que visa evoluir para alcançar a onnipresença.

Para melhor retratar esta vigilância complementar entre o digital e o mundo físico dos utilizadores, Mark Weiser previu esta realidade, intitulando-a de “computação ubíqua”, com a seguinte afirmação: “As tecnologias mais profundas são aquelas que desaparecem. Estas tecnologias entrelaçam-se no quotidiano até se tornarem indistinguíveis do mesmo.” (Weiser 1999 citado por Zuboff 2019b, 16). Esta abordagem reforça a ideia de que a internet se incorporará plenamente à rotina das pessoas, tornando-se indistinguível.

A natureza deste imperativo de extração, na abordagem do capitalismo de vigilância, reside na necessidade imperativa das empresas de acumular grandes volumes de dados comportamentais. Este imperativo é impulsionado pela dependência de algoritmos de aprendizagem automática, que requerem extensos conjuntos de dados para as previsões, e pela competição no mercado por informações cada vez mais refinadas que prometem lucros substanciais. A acumulação desta magnitude facilita o desenvolvimento de economias de escala. Isto é, adotando esta lógica as empresas conseguem obter uma redução de custos e um aumento da eficiência à medida que processam e analisam grandes volumes de dados, proporcionando vantagens competitivas ao realizar previsões mais precisas acerca do comportamento futuro dos indivíduos e adquirindo uma melhor compreensão dos seus utilizadores (Zuboff 2019).

1.4.2. O imperativo de previsão e as economias de âmbito

A acumulação de lucros provenientes da vigilância dos utilizadores intensificou a competitividade entre as empresas relativamente às receitas geradas com a aposta no novo mercado de “futuros comportamentais”.

Dado isso, segue-se a fase seguinte de intensidade competitiva - o imperativo de previsão. O volume de excedente comportamental, ainda que essencial para a contínua atuação dos capitalistas de vigilância, tornou-se insuficiente para o sucesso.

Considera-se que, os processos computacionais de transformação do excedente comportamental em produtos que preveem com precisão o futuro são tão eficazes quanto a qualidade dos dados disponíveis. Assim, uma vez que as empresas procuram a certeza na escolha dos utilizadores pelos seus produtos, tornou-se perceptível para as mesmas que as melhores previsões deveriam aproximar-se da observação direta do comportamento dos indivíduos. A realização acerca do poder de previsão representa outro marco relevante na cristalização do capitalismo de vigilância (Zuboff 2019).

A necessidade de uma observação direta do comportamento dos utilizadores assinala a transição para as economias de âmbito, isto é, o excedente comportamental deve ser, para além de extenso, diversificado. Mas, aqui, com economias de âmbito, procura-se o acesso aos padrões íntimos do “eu” do utilizador, como a tentativa de decifrar os significados de suspiros, pestanejos e falas (Zuboff 2019b, 17). A nova fonte de abastecimento de dados sobre o comportamento dos utilizadores visa a compreensão e futura previsão da personalidade, estados de espírito, emoções e vulnerabilidades dos indivíduos. Existe a dependência dos capitalistas de vigilância de um fluxo contínuo de dados, extensos e diversificados, que permitem chegar à certeza fabricada acerca dos “futuros comportamentais”, de modo a corresponder às exigências dos seus reais clientes: anunciantes.

A demanda pelo santuário interior do indivíduo, no contexto do capitalismo de vigilância, significa que o uso dos dados comportamentais vai para além da otimização da publicidade, através do capitalismo de vigilância as grandes empresas procuram desenvolver novos produtos, serviços personalizados, e até influenciar o comportamento dos utilizadores (Zuboff 2019b).

1.4.3. O imperativo de previsão e as economias de ação

As operações de abastecimento do capitalismo de vigilância representam uma arquitetura de métodos e instrumentos tecnológicos que permitem a contínua ação da lógica de acumulação aqui examinada: arquitetura da computação ubíqua (Zuboff 2019).

Através da nova arquitetura, desde dispositivos móveis, automóveis, ruas, estabelecimentos comerciais, a experiência humana no domínio digital e no mundo físico é continuamente extraída, transformada e convertida num produto do mercado de “futuros comportamentais” (Zuboff 2019).

De forma a suportar as operações de desenvolvimentos tecnológicos que até aqui garantem a ininterrupta recolha de dados comportamentais em larga escala, e garantem a análise preditiva do modelo de vigilância capitalista (como por exemplo, o financiamento de tecnologias, desenvolvimento de sistemas, armazenamento de dados, entre outros recursos), foi necessária uma crescente atração das receitas da vigilância - aumentando a intensidade competitiva do imperativo de previsão. Isto é, da mesma forma que, o volume de dados se tornou uma condição necessária, mas insuficiente para previsões mais alargadas e precisas da realidade dos utilizadores, também as economias de âmbito se tornaram insuficientes (Zuboff 2019b).

Ainda que essencial que o excedente comportamental seja extenso e diversificado, os capitalistas de vigilância perceberam gradualmente que a forma mais eficaz de prever o comportamento dos indivíduos é intervindo na origem do mesmo e moldá-lo às expectativas do mercado. Mais uma vez, a procura pela certeza acerca da escolha dos utilizadores é a máxima que garante às grandes empresas a contínua acumulação de capital. Os métodos desenvolvidos para alcançar esta máxima são o que a autora Shoshana Zuboff descreve como economias de ação, singulares do capitalismo de vigilância e o domínio do digital (Zuboff 2019).

Para alcançar as economias de ação, os processos e instrumentos tecnológicos automatizados são configurados para intervir no estado das coisas no mundo tangível. O resultado da execução das economias de ação é o aperfeiçoamento dos produtos preditivos. A execução das mesmas é possível seguindo os métodos de “afinação”, “condução”, e “condicionamento” do comportamento de indivíduos, grupos e populações (Zuboff 2019b).

Para cada um destes métodos de alteração de comportamentos, é possível apresentar alguns exemplos práticos. O método de “afinação” é uma abordagem que envolve a utilização de sugestões subliminares programadas que se apresentam aos utilizadores de forma a moldar, de forma subtil, isto é, fora da consciência humana, o fluxo de comportamento na hora e lugar exato para que a influência tenha o máximo de eficiência. Na sequência das tentativas dos capitalistas

de vigilância em programar a escolha dos utilizadores, a autora sublinha o conceito de: arquitetura da escolha. O conceito representa as formas por meio das quais situações já estão configuradas para canalizar a atenção e moldar a ação dos utilizadores. Um exemplo prático deste método é a inserção de uma frase ou slogan específico no *feed* do Facebook que encoraja a compra de algum produto ou serviço.

O método de “condução” é uma abordagem que se baseia no controlo de elementos essenciais no contexto imediato do indivíduo. Ao que a autora denomina de “o incontrolado”. Este método utiliza técnicas que orquestram de forma remota o contexto momentâneo do indivíduo, isto é, impedindo alternativas e, portanto, mudando o comportamento de acordo com um caminho de elevada previsibilidade que se aproxima de um comportamento “certo” que serve os objetivos da entidade que opera os recursos de vigilância. Um exemplo prático deste método é a capacidade atual de certas entidades, como por exemplo uma seguradora, de desligar o motor de um carro de um indivíduo que tenha o pagamento do seu seguro em atraso., isto é, ter controlo sobre o carro por meio de tecnologia que pode desligar o motor remotamente:

“A condução possibilita uma orquestração remota da situação humana, negando alternativas de ação e por conseguinte forçando o comportamento ao longo de um caminho de probabilidade crescente que se aproxima da certeza (...).”
(Zuboff 2019, 330).

Por último, o método de “condicionamento”, uma abordagem que introduz a aplicação de reforços, o que vai além dos modelos anteriores – um estímulo, uma resposta. A abordagem do condicionamento está associada ao behaviorista Burrhus Frederic Skinner (B. F. Skinner) e ao seu argumento de modificação comportamental, em que a mesma deve imitar o processo evolucionário na medida em que, certos comportamentos que ocorrem de forma natural são “selecionados” para o sucesso de uma determinada ação pelas condições do ambiente. Isto é, o projeto de “engenharia comportamental” pretende a modelação do comportamento para intensificar certas ações em detrimento de outras. Aplicando isto ao capitalismo de vigilância, a vantagem do condicionamento de ações está em determinar quais os comportamentos mais lucrativos para as empresas:

“O objetivo da nossa atividade é mudar o comportamento das pessoas em larga escala. Queremos descobrir como se constrói a mudança do comportamento de uma pessoa, e depois queremos mudar o modo como muitas pessoas tomam

decisões quotidianas. Quando as pessoas usam a nossa app, captamos os seus comportamentos e identificamos (...) bons e maus. Depois desenvolvemos “tratamentos” ou “grãos de dados” que escolhem comportamentos bons. Podemos testar quão acionáveis são as nossas pistas, para elas, e quão rentáveis serão, para nós, determinados comportamentos.” (Cientista de dados de uma empresa de educação de Silicon Valley citado por Zuboff 2019, 331).

Um exemplo prático deste método é o microdirecionamento comportamental a uma escala-populacional a partir de perfis do Facebook de forma a condicionar o voto dos indivíduos nas eleições norte-americanas de 2016. A empresa responsável por esta ação foi a Cambridge Analytica (Zuboff 2019).

1.5. Os 16 fatores impulsionadores do capitalismo de vigilância

O sucesso das economias de escala, de âmbito e de extração e, consequentemente o sucesso da lógica de mercado do capitalismo de vigilância deve-se a 16 fatores impulsionadores. A autora Shoshana Zuboff analisa as 16 razões que permitiram o desenvolvimento da lógica de acumulação de dados dos indivíduos.

O primeiro fator identificado é o ineditismo – pela razão das novas tecnologias de empresas como Google e Facebook beneficiarem da novidade das suas práticas, isto é, apresentarem no mercado produtos sem precedentes, a sociedade não estava preparada para reconhecer as implicações da sua utilização destes produtos. O “gosto” nas publicações do Facebook foi uma das derivações inéditas da empresa, no entanto, é uma das ferramentas de vigilância, por parte da empresa, dos seus utilizadores. Por norma, a atenção da população foca-se em reconhecer ameaças de vigilância e controlo associadas ao poder estatal (Zuboff 2019, 377).

O segundo fator é a ‘declaração de invasão’ – a empresa Google, pioneira na lógica de acumulação do excedente comportamental, reivindicou a recolha e análise de dados sem restrições prévias. Os dados dos utilizadores serviam como matéria-prima para garantir a acumulação de lucros. A declaração aberta da empresa do uso de dados para melhorar os seus produtos e serviços, através do registo de patentes, dos termos de serviço e políticas de privacidade, permitiu a institucionalização das práticas do capitalismo de vigilância: “Com base

nesta reivindicação, afirmamos ser nosso direito apropriarmos-nos da experiência pessoal para tradução em dados comportamentais.” (Zuboff 2019, 204 e 377).

O terceiro fator destacado na análise do capitalismo de vigilância é o contexto histórico em que se posiciona – o contexto neoliberal, nomeadamente em relação à internet e ao ciberespaço, e o contexto de crise vivido após os ataques de 11 de setembro de 2001 e a declaração de “Guerra ao Terror”, nos EUA. Dentro da perspectiva neoliberal, os EUA, como centro global da internet e sede de grandes plataformas digitais, promovem a autorregulação para manter a internet autónoma e livre. Esta dinâmica reflete-se na área de jurisdição pessoal, onde é determinado o alcance dos tribunais sobre as plataformas digitais e numa segunda área do direito, com a Seção 230 da Lei de Decência nas Comunicações²⁴, lei federal que concede imunidade geral às plataformas digitais e aos prestadores de serviços em relação à responsabilidade civil (Zang 2022, 10). O contexto de emergência securitária, num desenvolvimento paralelo, levou o Estado à procura das competências e tecnologias em rápido desenvolvimento, da Google e de outros capitalistas da vigilância em ascensão, desconsiderando preocupações e exigências com legislações sobre privacidade. A necessidade do Estado da aquisição destas competências e desenvolvimentos económicos gerou a criação de “afinidades eletivas” entre estas entidades, permitindo que as empresas tecnológicas prosperassem sem grandes restrições à sua atividade, e contribuindo para a promoção da tendência de um ‘excepcionalismo de vigilância’: “(...) que no rescaldo dos ataques do 11 de setembro se intensificaram as práticas de vigilância e os limites que havia até então foram derrubados (...). Esta viragem das atenções do poder e da política governamental após os ataques do 11 de Setembro em Nova Iorque e Washington, D.C., é a (...) condição histórica a abrigar o modelo de mercado inexperiente.” (Zuboff 2019, 133 – 134).

O quarto fator são as fortificações criadas pela Google em torno das cadeias de abastecimento de capital de vigilância, fortificações que protegeram o desenvolvimento e ampliaram o alcance da nova ordem económica do século XXI – empresas como a Google consolidaram a sua posição através de laços estreitos com políticos, ao mostrar a utilidade dos seus produtos e serviços para o processo eleitoral, contribuindo ainda para uma fácil transição de funcionários da Google para o governo: “A utilidade política da Google desbravou caminho para a porta giratória, invulgarmente apinhada e em rápida rotação, entre os centros de poder das costas leste e oeste.”; através da confusão deliberada de interesses públicos e privados, com o estabelecimento de relações e a atividade de lóbi e; através de uma “campanha intencional da

²⁴ Tradução livre de Communications Decency Act.

Google para influenciar o trabalho acadêmico e os debates culturais abrangentes, vitais para a formação das políticas, da opinião pública e da percepção política” (Zuboff 2019, 143-147).

O quinto fator corresponde ao ciclo de expropriação – iniciativas de empresas como a Google, por exemplo com o Google *Street View*, e de outras empresas líderes do capitalismo de vigilância, determinam os ritmos da expropriação dos dados dos utilizadores. As incursões na marca digital dos utilizadores são possibilitadas pela dinâmica complexa de relações com o setor público e o confronto jurídico que se destina a aproveitar tempo para a instalação de uma habitação gradual nos indivíduos, combatendo qualquer resistência que tenha sido demonstrada numa primeira fase aos produtos e iniciativas das empresas, ao que a autora refere como estratégias de adaptação (Zuboff 2019, 378).

O sexto fator identificado é o fenómeno da dependência dos indivíduos do meio digital e dos benefícios inerentes ao mesmo para o seu quotidiano – os serviços gratuitos oferecidos pelas empresas tecnológicas tornam-se indispensáveis para os indivíduos à medida que suprimiam necessidades, necessidades latentes à segunda modernidade (a partir das últimas décadas do século XX): conexão social, eficiência e conveniência, informação e conhecimento, reconhecimento e visibilidade, sentimento de segurança, maior participação e autonomia social e política, hoje os esses serviços estão integrados profundamente em várias formas de participação social, tornando difícil a rejeição ou desabituação:

“À medida que o capitalismo de vigilância se disseminou pela internet, as formas de participação social tornaram-se coextensivas com os meios de modificação comportamental. A exploração das necessidades da segunda modernidade que alimentou desde início o capitalismo da vigilância acabaria por impregnar todos os canais de participação social. Tornar-se-ia difícil rejeitar a sua utilidade e inclusive questionar a sua mera possibilidade.” (Zuboff 2019, 378-379).

O sétimo fator que Shoshana Zuboff aponta é a questão do interesse próprio: os novos mercados baseados em previsões do comportamento futuro dos utilizadores atraem uma rede de parceiros de vários setores de atividade, cujas receitas começaram também a depender do imperativo de previsão, como exemplo já referido são as localizações patrocinadas no mapa do jogo *Pokémon Go* (Zuboff 2019, 379).

O oitavo fator refere-se à inclusão – em linha com as necessidades da segunda modernidade, a tecnologia, redes sociais, plataformas de interação de modo geral vêm dar respostas. Atualmente, estar fora deste círculo cria o sentimento de exclusão, de perda de algo

importante, da não participação nos assuntos da sociedade. Isto é, a não-participação nestes motores de capital e informação é sinónimo de isolamento social (Zuboff 2019, 379).

O nono fator trata a identificação dos representantes das grandes empresas enquanto indivíduos empreendedores – existe uma admiração da sociedade perante o feito destes líderes tecnológicos enquanto indivíduos de sucesso financeiro e popularidade (Zuboff 2019, 379).

O décimo fator está ligado à autoridade imputada aos líderes das empresas, enquanto indivíduos visionários – em linha com a identificação dos representantes das grandes empresas enquanto indivíduos empreendedores, está a autoridade designada, por parte da sociedade, a estes mesmos indivíduos. Ou seja, o sucesso da empresa é razão para a legitimação da sua atuação pois a inovação tecnológica é associada, muitas vezes, a melhores perspetivas para o futuro dos indivíduos (Zuboff 2019, 379).

O décimo primeiro fator está ligado à persuasão social – para que haja uma maior aderência da sociedade às inovações tecnológicas que surgem, a autora identifica uma “retórica sedutora” que acompanha as novidades capitalistas, os eufemismos: publicidade direcionada, personalização, assistentes digitais. Assim, existe uma previsão e predeterminação de escolhas dos indivíduos, reforçando a lógica do capitalismo de vigilância (Zuboff 2019, 379).

O décimo segundo fator identificado pela autora é o fecho de alternativas aos indivíduos – em virtude da integração profunda das tecnologias de vigilância no quotidiano dos indivíduos, está presente uma exclusão de alternativas ao capitalismo de vigilância:

“O capitalismo de vigilância disseminou-se pela internet, e o uso de economias de âmbito e ação empurrou-o para o mundo real. Das apps para equipamentos às dedicadas à Voz Única, torna-se progressivamente mais difícil identificar formas de fuga, para não falar de alternativas genuínas.” (Zuboff 2019, 379-380).

O décimo terceiro fator corresponde à inevitabilidade – a tecnologia e a inovação tecnológica é, constantemente, explicada pela sua inevitabilidade. No entanto, como se verificou no início deste capítulo, a tecnologia está ligada a um processo de negociação entre o poder privado e o poder público, refletindo as agendas dos mesmos (Burgess 2010). Aqui, tal como indica a autora, é usada também uma retórica, a retórica da inevitabilidade da inovação. Contudo, tal como é explorado no livro de J.P. Burgess (2010), Shoshana Zuboff remete a tecnologia e os desenvolvimentos da mesma a um determinado contexto, num dado período. O capitalismo de vigilância é historicamente contingente (Zuboff 2019, 380). O argumento da inevitabilidade desvia

a atenção dos indivíduos das reais consequências da institucionalização do capitalismo de vigilância, levando a uma condescendência e aceitação resignada.

O décimo quarto fator remete para a ideologia da fraqueza humana – a convicção dos capitalistas de vigilância na vulnerabilidade das ações e percepções dos indivíduos é usada como motor de justificação para a contínua intervenção do capitalismo de vigilância no seu quotidiano. Aqui pode ser associada a psicologia do “outro”, adotada pelo psicólogo norte-americano B.F. Skinner, referido anteriormente quanto à sua abordagem - behaviorismo radical. A psicologia do “outro” sugere que o comportamento humanos só é compreendido cientificamente se os psicólogos observarem os humanos como “outros”, isto é, a “perspetiva do outro” é um requisito necessário para uma ciência objetiva do comportamento humano (Zuboff 2019, 380).

Após a adoção desta ideologia, B.F. Skinner produziu uma metodologia – ‘condicionamento operante’ – onde são determinados e moldados padrões de comportamento através de reforços específicos, isto é, com a introdução ou remoção de estímulos. Um reforço positivo envolve a apresentação de um estímulo agradável após um comportamento desejado, aumentando a frequência do comportamento. Enquanto um reforço negativo refere-se à remoção de um estímulo desagradável após a realização de um comportamento desejado, aumentando assim a probabilidade de que esse comportamento ocorra novamente (Zuboff 2019b, 21).

Diante a evolução das tecnologias de comportamento descritas, sugeridas por B.F. Skinner, são já parte integrante do capitalismo de vigilância, ao serem utilizados estímulos digitais para modificar e prever o comportamento humano em massa. Para reforços positivos inclui-se, por exemplo, aplicativos que utilizam sistemas de pontos ou recompensas virtuais, dessa forma incentivando à interação e participação contínua. Para reforços negativos inclui-se a oferta de certas funcionalidades adicionais e avançadas em aplicações, apenas para os utilizadores que completam determinadas ações, removendo também barreiras de uso (Zuboff 2019b, 22-23).

O décimo quinto fator está ligado à ignorância – a autora identifica que existe uma divisão anormal do conhecimento e da aprendizagem entre os capitalistas da vigilância e o resto da sociedade. Devido à “retórica sedutora”, aos eufemismos, aos secretismos, ao argumento da inevitabilidade e, principalmente, devido à ilegibilidade da sociedade sobre certos sistemas tecnológicos, esta lógica de acumulação progride e sai impune a restrições institucionais pelo facto de estar fora do alcance da compreensão da maioria dos indivíduos: “Estes sistemas pretendem seduzir-nos, saqueando as nossas vulnerabilidades criadas pela divisão de aprendizagem assimétrica e amplificadas pela escassez de tempo, de recursos e de apoio.” (Zuboff 2019, 380).

Em resultado da assimetria de conhecimento, a compreensão e a resistência eficaz às estratégias de vigilância ao capitalismo ficam inibidas.

O décimo sexto e último fator identificado por Shoshana Zuboff é a velocidade do desenvolvimento da nova ordem económica de vigilância - os sistemas tecnológicos têm, cada vez mais, um desenvolvimento rápido e difícil de acompanhar, que supera a capacidade da generalidade dos indivíduos em compreender como se chegou até esse desenvolvimento e quais as suas implicações reais para a sociedade. A autora entende esta estratégia de velocidade como uma forma consciente de impedir a resistência e a perceção dos indivíduos, e até do próprio Estado, dos desenvolvimentos tecnológicos que os capitalistas de vigilância introduzem, o que reflete um método de tentativa de controlo e dominação: “Esta estratégia nasce de um longo legado de abordagens políticas e militares à produção de velocidade como forma de violência, recentemente conhecida como ‘choque e pavor’ (Zuboff 2019, 380). E, ainda:

“As empresas de alta tecnologia andam três vezes mais depressa do que as empresas normais. E o governo anda três vezes mais devagar do que as empresas normais. Portanto, temos um intervalo de nove vezes (...) Logo, deve garantir-se que o governo não se intromete nem atrasa as coisas.” (Schmidt 2011 citado por Zuboff 2019, 125).

Perante estas condições de desenvolvimento da lógica do capitalismo, a autora sublinha a questão da dependência dos indivíduos face a plataformas como a Google e o Facebook. Com o avanço do capitalismo de vigilância, os meios de participação social ficaram condicionados aos métodos de ação da nova lógica de mercado. Ou seja, os meios de participação social tornaram-se indissociáveis dos métodos de modificação comportamental, debilitando os instrumentos de escolha que fazem parte da esfera privada – “saída”, “voz” e “lealdade”. Isto é, não há forma de evitar estes métodos de modificação comportamental se não for possível detetá-los previamente. Para além disso, a falta de “voz” ou expressão dos utilizadores remete para o facto de, tal como a palavra indica, utilizadores são os consumidores e não os clientes destas plataformas e, por essa razão, carecem de formas institucionais para uma ação coletiva efetiva, onde também haja a garantia de um canal de expressão confiável. De forma semelhante para a noção de “lealdade”, que é desprovida de fundamento uma vez que, a contínua participação dos indivíduos é interpretada como uma falta de alternativas à opção capitalista, o que reflete uma impotência face à realidade e, consequentemente, a noção de impotência leva a uma aceitação resignada e à condescendência perante o contexto de mercado referido (Zuboff 2019b, 23).

Analisados os 16 fatores que levaram ao sucesso do capitalismo de vigilância, o passo seguinte da autora passa por perceber de que forma o capitalismo de vigilância consegue perdurar no tempo. A resposta está na análise do poder adjacente a esta lógica de acumulação de dados dos indivíduos, ao qual intitula de “poder instrumentarista”.

1.6. O poder ‘instrumentarista’ do capitalismo de vigilância

O poder adjacente ao capitalismo de vigilância é um poder também ele inédito – uma espécie de poder sem precedentes que surge perante uma nova lógica de mercado, o capitalismo de vigilância, lógica que se baseia na desapropriação do comportamento humano para completar a sua ambição de lucro,

“(…). Qualquer encontro com o inédito é, por si mesmo, um verdadeiro desafio intelectual e existencial, e este facto merece a nossa atenção. O inédito é necessariamente irreconhecível, tacitamente interpretado através da lente das categorias familiares. Esta operação mental torna invisíveis precisamente as dimensões da experiência para as quais não existem configurações mentais estabelecidas.” (Zuboff 2019b, 24)²⁵.

De forma a comparar o ineditismo entre poderes, Soshana Zuboff remonta ao aparecimento do totalitarismo como uma nova forma de poder. No entanto, adverte que, para uma resistência eficaz ao poder apresentado pelo capitalismo de vigilância, é necessário utilizar uma nova lente de observação e interpretação dos seus mecanismos de ação, ao invés de utilizar a lente de observação do totalitarismo para o classificar, tal como o uso de noções como “totalitarismo digital” ou “o Grande Irmão” (Zuboff 2019b, 25-28):

“O totalitarismo pretendia a purificação da espécie humana através dos mecanismos de genocídio e da “engenharia da alma”. (...) Mas comandar populações até à sua alma exige um esforço inimaginável, o que era uma das razões pelas quais o totalitarismo era inimaginável. (...) A vida interior de cada um deve ser reivindicada e transformada pela ameaça perpétua de terror: castigo sem crime. Este trabalho meticuloso requer a orquestração

²⁵ Tradução livre de: Any encounter with the unprecedented is itself a genuine intellectual and existential challenge, and this fact itself merits our attention. That which is unprecedented is necessarily unrecognizable, tacitly interpreted through the lens of familiar categories. This mental operation renders invisible precisely those dimensions of experience for which there are no established mental sets.

pormenorizada de isolamento, ansiedade, medo, persuasão, fantasia, desejo, inspiração, tortura, pavor e vigilância.” (Zuboff 2019b, 27)²⁶.

O capitalismo de vigilância apresenta-se também, como uma nova ordem económica que se apoia na vigilância dos dados dos indivíduos e garante o lucro através dessa vigilância, com o objetivo final da modificação do comportamento dos indivíduos para comportamentos mais lucrativos para as empresas. Novos desafios e novos perigos – revogação do direito à privacidade, do direito a ter direitos (Zuboff 2019b, 35)²⁷.

A nova espécie de poder “instrumentarista” apoia-se em dois mecanismos que permitem a modificação, previsão, monetização e controlo do comportamento dos indivíduos: “instrumentar” e “instrumentalizar” o comportamento. O credo do capitalismo de vigilância, ao contrário do totalitarismo, é a “engenharia do comportamento”, uma visão baseada no behaviorismo radical de B.F. Skinner. O poder “instrumentarista” assenta no ponto de vista do “outro”, ponto de observação do behaviorismo radical para a observação do comportamento de outros organismos. Assim, as relações sociais e trocas económicas ocorrem, no contexto da ordem económica do capitalismo de vigilância, através deste véu automatizado de abstração: a “perspetiva da visão divina”: “(...) usar um olhar distante e desprendido (...)” (Zuboff 2019, 461).

A visão indiferente adotada pelos capitalistas de vigilância em relação ao indivíduo é atingida por meio dos aparelhos digitais de computação ubíqua. Shoshana Zuboff encara esse conjunto de aparelhos e sistemas digitais como um todo, um aparelho ubíquo, ao qual intitula de “o Grande Outro”, desde os smartphones onnipresentes, assistentes virtuais como Amazon Alexa e Google Home, câmaras de segurança e campanhas inteligentes, carros conectados até às redes sociais e serviços de pesquisa como a Google. A posição de “indiferença radical” em relação à experiência humana é resultado das capacidades do “Grande Outro” em tornar essa mesma experiência em comportamentos mensuráveis e observáveis, permitindo aos capitalistas de vigilância manterem-se firmemente indiferentes ao significado dessa experiência humana:

²⁶ Tradução livre de: Totalitarianism was bent on the purification of the human species through the dual mechanisms of genocide and the “engineering of the soul.” (...) But to command populations right down to their souls requires unimaginable effort, which was one reason why totalitarianism was unimaginable. (...) Each individual inner life must be claimed and transformed by the perpetual threat of terror: punishment without crime. This craftwork requires the detailed orchestration of isolation, anxiety, fear, persuasion, fantasy, longing, inspiration, torture, dread, and surveillance.

²⁷ A privacidade é um direito epistémico, mas o direito à privacidade, isto é, o direito de escolher manter informações pessoais privadas, é um direito fundamental. O direito fundamental que engloba não apenas o controlo sobre informações pessoais, mas também a proteção contra invasões à vida privada e à autonomia individual, o que garante aos indivíduos espaço para agir livremente e sem coerção externa (Zuboff 2019b)

“Treinado em ações mensuráveis, o Grande Outro importa-se apenas com a observação do que fazemos e com garantir que façamos isso de formas acessíveis às suas operações de interpretação, reforço, cálculo e monetização. A indiferença radical do poder instrumentarista é operacionalizada nos métodos desumanizados de avaliação do Grande Outro, que produzem equivalência sem igualdade ao reduzir os indivíduos ao menor denominador comum de mesmice – um organismo entre organismos.” (Zuboffb 2019b, 30)²⁸.

Ambas as espécies de poder, totalitarismo e o instrumentarismo, têm um visão totalista da experiência humana, no entanto, são visões totalistas diferentes e com finalidades diferentes. Concernente ao totalitarismo, a visão totalista passa pela pretensão de uma posse total dos indivíduos, e das suas almas, pela reeducação dos mesmos para a lealdade absoluta através da subjugação ao Estado. O centro de poder passa pelo controlo dos meios de violência, exercendo ao mesmo tempo uma aplicação hierárquica do terror, constituindo o terror arbitrário um mecanismo fundamental do totalitarismo. No que tange ao poder instrumentarista, a visão totalista passa pela pretensão de uma certeza total acerca dos comportamentos dos indivíduos, pela modificação comportamental dos mesmos através do alcance da transparência absoluta por meio das capacidades da computação ubíqua. O centro de poder passa pelo controlo da divisão da aprendizagem na sociedade, atingida pela propriedade dos capitalistas de vigilância dos meios de modificação comportamental. A expropriação de excedente comportamental para computação, controlo, previsão do comportamento dos indivíduos constitui um mecanismo fundamental e imprescindível para a finalidade do poder instrumentarista - a automação do mercado/sociedade para a certeza dos resultados garantidos (Zuboff 2019, 436-437).

Ainda que espécies de poder totalistas diferentes, ambas sem precedentes nas suas respetivas eras. Assim, o capitalismo de vigilância, inédito nas suas capacidades e métodos de atuação, no século do digital, apresenta novos desafios ao combate dos excessos da nova lógica de mercado. A velocidade da inovação e da circulação da informação, ainda que um fator atrativo, representa também uma dificuldade para as instituições e organismos que pretendem regular a atuação das empresas motoras do capitalismo de vigilância:

²⁸ Tradução livre de: Trained on measurable action, Big Other cares only about observing what we do and ensuring that we do it in ways that are accessible to its ever-evolving operations of rendition, reinforcement, calculation, and monetization. Instrumentarianism's radical indifference is operationalized in Big Other's dehumanized methods of evaluation that produce *equivalence without equality* by reducing individuals to the lowest common denominator of sameness – an organism among organisms.

“Estas plataformas constituem uma verdadeira mudança de paradigma, semelhante à invenção da televisão, e o que lhes confere poder é a sua capacidade de evoluir, mais concretamente, a velocidade com a qual se expandem. Quase nada, a não ser um vírus biológico, pode propagar-se com tanta rapidez, eficiência ou agressividade quanto as plataformas tecnológicas, o que torna as pessoas que as constroem, controlam e utilizam também elas poderosas.” (Schmidt, e Cohen 2013, 9-10)²⁹.

Além da velocidade inédita, as concentrações de conhecimento são também elas, inéditas. As empresas tecnológicas têm acesso a uma diversidade de informação sem precedentes. Com a “instrumentação” da arquitetura tecnológica onnipresente e a “instrumentalização”, por meio dessa arquitetura tecnológica, das relações sociais que caracterizam a experiência humana através da sua observação próxima, as empresas conseguem transformar a experiência humana numa mercadoria lucrativa. A combinação da “instrumentação” e “instrumentalização” circunscreve o poder “instrumentarista” que define e orienta a aplicação prática das estratégias da lógica de mercado do capitalismo de vigilância (Zuboff 2019b).

A empresa escolhida para o estudo de caso desta dissertação, *Palantir Technologies*, é analisada à luz das principais características do capitalismo de vigilância. No entanto, prossegue-se, primeiramente, à contextualização da conjuntura internacional em que surge a empresa.

Capítulo II. A nova conjuntura (inter-)nacional e a emergência de *Palantir Technologies*

2.1. A nova conjuntura (inter-)nacional: 11 de setembro e o advento do *intelligence-led policing*

Como já foi estabelecido no início desta dissertação, a 11 de setembro de 2001, os EUA foram alvo de um conjunto de ataques terroristas que iriam afetar a percepção e ação sobre a sua segurança, voltando-se para a vigilância massificada dos dados dos indivíduos de forma a conseguir prever instâncias congêneres. De modo a aprofundar este argumento, este capítulo analisa em maior detalhe a evolução na utilização da vigilância de dados.

A investigação nesta dissertação está direcionada para a aposta por parte dos EUA na vigilância dos dados da população no âmbito de *policing*, atividade ligada aos departamentos de

²⁹ Tradução livre de: These platforms constitute a true paradigm shift, akin to the invention of television, and what gives them power is their ability to grow – specifically, the speed at which they scale. Almost nothing short of a biological virus can spread as quickly, efficiently or aggressively as these technology platforms, and this makes the people who build, control and use them powerful too.

law enforcement nos EUA, procurando atender no seguimento deste capítulo às seguintes subquestões: O que despertou no Estado norte-americano o seu novo foco na vigilância dos dados dos indivíduos? E quais foram as razões que levaram ao papel revigorado dos departamentos de *law enforcement*?

Para o desenvolvimento da dissertação torna-se necessário nesta fase da investigação aprimorar o conceito de vigilância. Dessa forma, temos que é consensual nos estudos de vigilância, que o conceito, tendo em conta a raiz e etimologia da palavra³⁰, já se fazia sentir ao longo do último século: “a prática da vigilância abrange a recolha, o gravar e o classificar de informação sobre pessoas, processos e instituições”³¹, mas a noção de vigilância enquanto prática remonta pelo menos ao século XVI com o desenvolvimento de um estado-nação e do comércio transatlântico de escravos (Foucault 1977; Haggerty e Ericson 2000; Lyon 2003; Marx 2016 citados por Brayne 2017, 978). No entanto, o que se verifica é uma orientação diferente da mesma nas últimas décadas vis-à-vis o acontecimento chave dos ataques de 11 de setembro de 2001, ponto de viragem na história de vigilância dos EUA. Orientação que promove uma variação associada aos novos termos da vigilância que se encontra vinculada ao conceito de *intelligence*³².

Aquando da análise da bibliografia mais recente, surge uma ligação do conceito de vigilância ao conceito de *intelligence*, tal como referido, por efeito de um desenvolvimento nos instrumentos utilizados no comando dessa vigilância: através de um alinhamento entre os atores interessados na prática desta vigilância por meio de uma partilha de informações e de uma convergência entre sistemas de vigilância anteriormente separados para um aglomerado de sistemas conectados, uma *surveillant assemblage* (Deleuze and Guattari 1987; Haggerty and Ericson 2000 citados por Brayne 2017, 978).

De forma a contextualizar, verificamos no período após os eventos do 11 de setembro, cujo acontecimento é entendido como um malogro na história dos EUA, o levantamento de questões sobre a hegemonia dos EUA, bem como sobre a sua capacidade em providenciar segurança a outros Estados, papel geralmente atribuído aos EUA pela comunidade internacional. No entanto, de modo a enfrentar esta perturbação na segurança nacional, os EUA adotaram uma posição reacionária que respaldava uma diretiva trazida pelo sentimento de instabilidade,

³⁰ Etimologia da palavra vigilância: derivada do latim *vigilantia*, de *vigilare* - tomar conta, observar atentamente.

³¹ Tradução livre de: The practice of surveillance involves the collection, recording, and classification of information about people, processes, and institutions.

³² *Intelligence* é um conceito entendido como o produto final do processo de pesquisa de dados (brutos), processo que envolve posteriormente a contextualização das informações adquiridas e de uma avaliação do risco de modo que esta *intelligence* se torne útil na prática (Brayne 2017).

Homeland Security Act, diretiva que requisitava a concentração em todas as unidades de segurança nacionais, que passíveis de terem um contacto com a nova realidade internacional: o terrorismo transnacional, se mostrariam relevantes no combate ao mesmo e na reposição do sentimento de segurança.

Assim, numa necessidade de reorientação de estratégias, os EUA apostavam em investimentos volumosos nas suas unidades e agências de segurança, incluindo os departamentos de *law enforcement*³³, que ainda que se possam caracterizar como parcelas exíguas em relação à sua atividade e importância formam uma parceria estratégica com a Comunidade de Inteligência dos EUA (CI) na segurança do país:

“(...) A Comunidade de Inteligência e os seus parceiros responsáveis pela aplicação da lei fizeram progressos significativos desde o 11 de setembro na criação de capacidades, na normalização de práticas e na partilha de informações com parceiros de missões nacionais nos Estados Unidos para se defenderem e responderem a ameaças estrangeiras e de inspiração estrangeira à nossa pátria. Muitas ameaças aos EUA – como as representadas por terroristas e grupos de crime organizado transnacional – ultrapassam fronteiras, tornando este tipo de cooperação uma necessidade.” (Office of the Director of National Intelligence 2017.)³⁴.

É, então, no contexto adjacente ao clima de insegurança, que foram sendo atribuídos às várias unidades policiais locais, os departamentos de *law enforcement*, fundos para que se pudessem requalificar e redirecionar com sucesso para a preempção e prevenção no combate ao terrorismo, constituindo assim ao lado da CI, as agências de segurança na linha da frente nacional na contenda com o terrorismo iminente. Com a diretiva do *Homeland Security Act* de 2002 estavam a ser disponibilizados fundos num valor estimado de 17 biliões de dólares aos Estados federados e governos locais para financiarem os seus departamentos de *law enforcement*, fundos que estavam atrelados a uma diretriz de comando:

³³ Os departamentos de *law enforcement* englobam todas as agências governamentais do aparelho securitário dos EUA. Por esse motivo e, pelo facto do termo mais aproximado em português – aplicação da lei – ser muito inconclusivo relativamente ao termo, a expressão é utilizada em inglês na presente dissertação.

³⁴ Tradução livre: The IC and its law enforcement partners have made significant progress since 9/11 in building capacity, standardizing practices, and sharing information with domestic mission partners in the United States to defend against and respond to foreign and foreign-inspired threats to our homeland. Many threats to the U.S. – such as those posed by terrorists and transnational organized crime groups – transcend borders, making this type of cooperation a necessity.

“O Subsecretário para a Análise da Informação e Proteção das Infraestruturas terá as seguintes funções: (1) aceder, receber e analisar informações de *law enforcement*, informações provenientes de *intelligence*, e outras informações de agências do Governo Federal, agências governamentais estaduais e locais (incluindo agências de *law enforcement*) e entidades do setor privado, bem como integrar essas informações de maneira a que seja possível – (A) identificar e avaliar a natureza e o âmbito das ameaças terroristas à pátria; (B) detetar e identificar ameaças de terrorismo contra os Estados Unidos; e (C) compreender essas ameaças à luz das vulnerabilidades reais e potenciais do território nacional.” (Departamento de Segurança Interna dos EUA 2002, 119)³⁵.

Verificou-se, neste período temporal, uma aceleração no processo de reunir uma vasta quantidade de informação que diversa, extensa e rápida (*BigData*) é analisada e contextualizada de modo a ser aplicada na prática, à luz da realidade vivida pelos departamentos de *law enforcement*. Isto é, aplicando o uso de *intelligence* à atividade destes departamentos assiste-se a uma nova dinâmica de *policing* que chega com o pós-11 de setembro.

Com a introdução do conceito de *intelligence* na abordagem do *policing*, os departamentos de *law enforcement* adquiriram capacidades acrescidas em termos de reunião dos factos e a capacidade de anteceder possíveis desfechos conjecturados por ameaças terroristas. Isto foi possível através do acesso a estas informações privilegiadas, transitando assim para um *predictive policing*³⁶ que angaria para estas agências um poder de previsão sobre acontecimentos futuros.

Percebe-se, neste contexto, que não foi um processo moroso para que os EUA entendessem os aspetos positivos e as contribuições que advinham da aquisição desta natureza de informação acerca da vida de pessoas, organizações, instituições, de locais e situações, o que se tornaria, como se irá analisar posteriormente nesta dissertação, numa prática comum e ampla

³⁵ Tradução livre de: Under Secretary for Information Analysis and Infrastructure Protection shall be as follows: (1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to— (A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland.

³⁶ Verifica-se, na análise qualitativa da bibliografia, pontos em comum na definição do que é *predictive policing*: o uso de técnicas analíticas de dados que passam por métodos tecnológicos e algorítmicos que circunscrevem a atividade criminal ao nível espacial/local e ao nível do indivíduo/conjunto de indivíduos de modo a prever a ocorrência da mesma, ou de forma a estabelecer uma rota que reúna os vários conjuntos de dados com base numa recolha no “terreno” e de uma análise humana que irá contextualizar os dados. Este processo tem como objetivo o reverter prático e efetivo nas estatísticas de crime ao diminuir a ocorrência do mesmo nas cidades (Brayne, e Christin 2020; Egbert 2019; Richardson et al. 2019). É escolhida para esta dissertação, a utilização do conceito de *predictive policing* em inglês, pelos mesmos motivos do uso do termo *policing* (ver nota de rodapé 3).

para este Estado. É com a ajuda de um setor privado tecnológico, disposto a ceder as suas capacidades, que esta reunião de informações se torna possível, procurando também este setor, por sua vez, garantir uma lógica de capitalização de informação. Verifica-se, atualmente, que o uso de *intelligence* e a utilização do *predictive policing* são práticas alargadas a outros Estados e empresas pelo mundo, pelo receio e pela iminência do terrorismo transnacional e as novas ameaças criadas com o desenvolvimento da tecnologia, como exemplo os ciberataques, tornando-se a utilização destas técnicas um panorama internacional.

A aposta recente e crescente, pelos departamentos de *law enforcement*, numa modalidade de vigilância na base da recolha e análise de dados foi transformando o processo de tomada de decisão com a adoção de uma metodologia *data-driven*, orientado para os dados.

Não é acolhida aqui, a ideia de que a utilização de dados e análise de estatísticas não existia previamente ao 11 de setembro. Esta utilização remonta ao século XX, pelo menos no âmbito do sistema de justiça penal, uma vez que era estudada a possibilidade de haver criminosos reincidentes e, por isso, tornou-se um imperativo para os tribunais avaliar o risco destas pessoas e do evento de novos crimes. Assim, foi introduzido no sistema de justiça criminal o método *actuarial justice*, isto é, onde os atores responsáveis faziam uma análise do risco e a sua gestão para medir a possibilidade de ocorrência de novos crimes (Brayne 2017, 981).

O cálculo do risco e a gestão do mesmo foram métodos de *actuarial justice* que avançaram para os departamentos da polícia nos EUA. O que tinha começado em 1994, com o *CompStat* no departamento da polícia de Nova Iorque, foi um dos primeiros passos para a realidade incursa que vivemos hoje de um *social sorting* sugerido por David Lyon, isto é, com a categorização de pessoas em diferentes grupos de modo a estabelecer juízos de valor e discernir resultados (Lyon 2007, 168). *CompStat* é um modelo criado para o mapeamento do crime, fazendo a correlação entre as estatísticas de criminalidade e a fiscalização da mesma de modo a identificar padrões nos crimes e a direcionar os recursos das unidades de segurança para áreas problemáticas identificadas pelos responsáveis. Verifica-se também, nesta transição, uma substituição de métodos e técnicas usadas pelos departamentos da polícia, mudanças estas que tornariam o modelo de patrulha policial mais eficaz e pró-ativo ao invés de uma posição reativa que liderou durante anos (Brayne 2017, 981).

Assim, a conjuntura internacional de instabilidade e insegurança, que se verificou após os ataques do 11 de setembro, trazia uma urgência às agências de segurança dos EUA na sua requalificação e modernização, com a integração de metodologias orientadas pelos dados que

permitiam uma avaliação e gestão de riscos. Essa conjuntura levou a que fosse empreendida a prática de um *intelligence-led policing*, com a contínua aposta na pesquisa e processamento de dados e com o contínuo desenvolvimento dos instrumentos tecnológicos e algorítmicos.

Advém, então, desta conjuntura, um incentivo à institucionalização das metodologias orientadas por dados e ao *intelligence-led policing*. Ainda assim, a transição e o desenvolvimento dos instrumentos de tecnologia avançada são contínuos, inclusive com o recurso e progressão para os *black-boxed algorithms* (algoritmos de caixa-negra):

“O algoritmo não é constituído apenas por uma componente abstrata e imaterial de ‘lógica’, mas também, por via de um conjunto de mecanismos de ‘controle’ é capaz de uma autorrealização no mundo - uma ecologia de sensores e software, corpos e burocracia, hardware e minerais (Munn s.d)³⁷.”

Com o desenvolvimento da tecnologia e com a transição da ação dos responsáveis pela segurança do país para uma posição mais pró-ativa no combate ao crime, mais prementemente, na prevenção e combate ao terrorismo, processa-se na história dos departamentos de *law enforcement* um conjunto de incentivos que partem do Governo Federal, para além do já referido *Homeland Security Act*. Com grande expressão para estes departamentos temos o projeto *Smart Policing Initiative*³⁸, que representa um conjunto de fundos fornecidos a estas unidades de segurança para que desenvolvam e adotem o uso progressivo de tecnologia e optem por uma análise preditiva através do recurso à mesma (Brayne 2017).

Palantir Technologies é uma das empresas com maior expressão neste auxílio aos departamentos de *law enforcement*, tal como se irá abordar no capítulo seguinte desta dissertação com a análise da cooperação estreita entre *Palantir Technologies* e o Departamento da Polícia de Los Angeles, entre *Palantir Technologies* e o Departamento da Polícia de Nova Orleães, e entre *Palantir Technologies* e a agência governamental *ICE*. Inclui-se aqui também esta última agência pois existiu uma cooperação estreita entre a empresa referida e esta agência devido ao desafio que se colocou nas questões imigratórias com o mandato do presidente Donald Trump.

³⁷ Tradução livre de: The algorithm is not just composed of an abstracted and immaterial ‘logic’ component, but also the ‘control’ mechanisms which carry out its work in the world—an ecology of sensors and software, bodies and bureaucracy, hardware and minerals.

³⁸ *Smart Policing Initiative* (2009/2010) é o nome dado à iniciativa criada por um consórcio entre o *Bureau of Justice Assistance* (BJA), os departamentos de polícia local e investigadores que resultou num aglomerado de fundos a mais de 30 departamentos, que incluía o DPLA, e servia de impulso na adoção a novas práticas ligadas ao *predictive policing* (Brayne 2017, 981).

Ainda que as cooperações referidas tenham ocorrido anos após o 11 de setembro, percebe-se aqui a dinâmica que liderou a ação dos departamentos da polícia e das próprias agências governamentais: a aposta no *intelligence-led policing* e no *predictive policing*, que partiu do receio de novos ataques terroristas como os vividos nessa data nos EUA, ao colaborar com o setor privado, número um no campo tecnológico. De forma a analisar como se processaram estas cooperações com *Palantir Technologies* é necessário compreender primeiro, ainda neste capítulo, de que modo *Palantir Technologies* se destacou neste contexto de insegurança, devido às suas capacidades, e a emergência na utilização dessas mesmas capacidades por parte das agências de segurança dos EUA, para a modernização e requalificação das últimas.

2.2. A emergência de *Palantir Technologies*: uma visão geral

Palantir Technologies, uma empresa de software norte-americana, situada inicialmente em Silicon Valley, no epicentro da tecnologia avançada e inovação, hoje encontra-se em Denver, Colorado nos EUA . Esta empresa comporta o estudo de caso desta dissertação, de modo que seja possível perceber de que forma o capitalismo de vigilância aqui estudado se aplica a uma das grandes empresas de *data-mining* ligadas à atividade do Estado, desde a sua fundação em 2004.

Os principais fundadores da empresa são Peter Thiel, Alex Karp, Stephen Cohen, Nathan Gettings e Joe Lonsdale, sendo que Alex Karp representa a figura de *CEO, Chief Executive Officer* e Peter Thiel, *Chairperson*. Peter Thiel e Alex Karp são as figuras representativas da empresa e, por esse motivo torna-se relevante associá-las às suas orientações políticas e ideais. Peter Thiel, um republicano e conservador com uma agenda que apoiava o *Political Action Committee (PAC)*: “*Make America Number 1*” enquanto, Alex Karp encontra-se do outro lado do espectro como socialista e progressista, rejeitando figuras como Donald Trump (Thomas 2022). No entanto, Alex Karp, o maior representante da empresa na esfera pública, toma uma posição vincada sobre o apoio que a empresa, *Palantir Technologies*, irá dar, continuamente, ao governo e exército norte-americano em matéria de tecnologia. Este último é um forte defensor de que o governo norte-americano deve ser o número um, ao nível dos Estados, na componente tecnológica e na inteligência artificial (Palantir Technologies 2020b).

O nome da empresa está ligado a uma referência ao filme: “O Senhor dos Anéis”, uma vez que “*Palantír*” se refere a uma bola de cristal que é usada para comunicação e para visualizar o que se passa noutros pontos da Terra. Trata-se de uma escolha do nome que reflete as

capacidades e funções da empresa, análise de dados e, nomeadamente a integração e visualização de dados através do seu software. Isto é, a empresa consegue proporcionar o acesso e a análise dos dados que pertencem a diferentes fontes, ao mesmo tempo que fornece uma visão integral dos mesmos, facilitando assim a compreensão e processo de análise aos seus utilizadores (Iliadis e Acker 2022, 338).

Desde a sua criação, *Palantir*, financiada pela empresa de capital de risco *In-Q-Tel*, da Agência Central de Inteligência (CIA), esteve ligada à Comunidade de Inteligência dos Estados Unidos (CI)³⁹ e na sua evolução assim o continua a fazer, paulatinamente. No entanto, vemos um repertório de instâncias em que a empresa proporcionou o seu software enquanto serviço de apoio a departamentos de *law enforcement* norte-americanos, mas, também, a empresas privadas e a outros governos estrangeiros, como é o caso do Reino Unido (Privacy International 2020). *Palantir Technologies* detém, também, um conjunto de empresas subsidiárias pelo mundo. Apesar da sua sede norte-americana, os seus serviços e capacidades tecnológicas são requeridas, também, no seio da Europa (Iliadis e Acker 2022, 336).

Os principais projetos e produtos desenvolvidos pela empresa são: Palantir Apollo; Palantir Gotham e Palantir Foundry. Estes atribuem à empresa um valor acrescentado, no que diz respeito ao fornecimento de um software que integra dados bem como a sua análise, dados estes de redes, plataformas e entidades públicas e privadas diferenciadas. Apollo é a plataforma base que atualiza e suporta os restantes produtos, nomeadamente, Gotham “The Operating System for Global Decision Making” (Palantir Technologies s.d.), e Foundry, “The Central decision support infrastructure for any organization” (Palantir Technologies 2021). Gotham é um produto mais direcionado para a área da defesa e de suporte à tomada de decisão junto de governos, enquanto o produto Foundry centra-se no apoio a organizações e a empresas para a organização dos seus dados. A empresa faz uma demonstração pública da organização e utilização destes produtos pela empresa, no entanto, com muito pouco detalhe como podemos ver no **Anexo I**.

No seio do Federal Procurement Data System é possível ter uma visão dos contratos que *Palantir Technologies* já teve com entidades públicas, isto é, com agências governamentais do Estado norte-americano. Apesar dos principais contratos e os mais lucrativos serem aqueles

³⁹ Lista de contratos de *Palantir Technologies* com agências governamentais, pelo Federal *Procurement Data System*, um repositório de consulta de milhões de ações contratuais federais: <https://www.fpds.gov/ezsearch/search.do?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir&renderer=isp&length=1274>; Lista de contratos mais recentes, 2022-2023: <https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir+2023&renderer=isp&length=130>

diretamente ligados ao exército norte-americano e à CI dos Estados Unidos, existem também contratos entre *Palantir Technologies* e os departamentos de *law enforcement* deste país. Ainda que o número de parcerias contratuais entre departamentos de *law enforcement* norte-americanos e *Palantir Technologies* seja residual, a análise do desenvolvimento dessas mesmas parcerias é crucial para perceber os termos em que segue a cooperação entre as partes (o exato número de parcerias contratuais entre as partes referidas não pode ser determinado, uma vez que não é divulgado publicamente por motivos de confidencialidade).

Apesar do foco desta dissertação estar na conjuntura do *policing*, identifica-se o percurso da empresa no seu todo relevante, tendo em conta que, o apoio ao Estado é recorrente e transversal às várias agências do governo. O percurso que começou com o objetivo de apoiar de perto os EUA no âmbito militar, passou pelo apoio a autoridades policiais locais e a várias outras agências governamentais norte-americanas que fazem parte, também, da CI, para além de contratos com outras empresas privadas e mais, recentemente, verificamos a aposta numa plataforma de defesa com recurso à inteligência artificial.

De modo a trazer um valor acrescentado à dissertação, a investigação incluiu a entrevista realizada com um representante da empresa *Palantir Technologies* no dia 24 de maio de 2023, previamente agendada através da troca de emails. A entrevista teve como objetivo refletir sobre as questões fundamentais ao estudo de caso já referidas e, de forma geral, contribuiu para registar a posição de *Palantir Technologies* sobre as eventualidades que se verificaram acerca das parcerias entre o Estado e o setor privado de software. A pedido do representante de *Palantir Technologies*, as observações destacadas em análise à entrevista realizada, seguem no anonimato, podendo desta forma ser integrada na dissertação.

Assim sendo, à luz das cooperações no seio de *law enforcement*, é possível verificar que o software da empresa tem licença e que os termos destas parcerias com *law enforcement* são sempre na base da negociação. A juntar a isto, é declarado publicamente pela empresa que, em nenhuma circunstância existe a apropriação e o armazenamento dos dados destes clientes por parte da companhia. Na visão da empresa existe um entendimento de que é realmente necessário haver uma cooperação maior entre o Estado e o setor privado de forma a acompanhar a evolução e, de modo a colmatar certos desafios que se apresentam na ação deste ramo de atividade do governo, entre os quais: investigações na área da cibersegurança, o combate a ameaças cibernéticas. Para que *law enforcement* detenha as ferramentas adequadas aos desafios que se apresentam atualmente é importante a satisfação da exigência de métodos sofisticados e

atualizados que dê resposta à necessidade. Para além disso, as exigências desta natureza que se colocam às entidades governamentais necessitam de um nível de conhecimentos especializados que são garantidos por empresas como *Palantir Technologies*, uma vez que, as agências aqui em questão não têm a capacidade nem os recursos para desenvolver uma plataforma própria de software que corresponda à procura que se manifesta, esta perceção confirma-se na entrevista (Entrevista realizada a um representante de *Palantir Technologies* 2023).

Palantir Technologies destaca-se, em relação a outras empresas do ramo, ao nível das suas capacidades analíticas pela aposta na sua plataforma de integração de dados, que organiza e aglomera vários sistemas de dados das instituições de *law enforcement*, anteriormente fechados e isolados. Para além de que, a sua base de dados incorpora dados de outras plataformas do Estado e suas diferentes instituições, criando uma única plataforma que permita a integração e visualização de toda esta informação, tornando-a disponível e simplificada ao cliente.

De acordo com o representante de *Palantir Technologies*, com a utilização da plataforma referida existe a garantia de *accountability* (responsabilidade por), ao ser capaz de monitorizar e combater qualquer tentativa de terceiros no acesso a estas informações e ao seu sistema. Ou seja, *Palantir Technologies* destaca-se pelas suas capacidades distintivas em fazer a referência e verificação cruzada de informação distribuída por vários sistemas, o que é um ponto fulcral para a ação destes departamentos. Ademais, acresce o facto do seu software conseguir emitir alertas para quaisquer novas informações que possam ajudar a prosseguir com uma investigação em curso ou, até mesmo, reunir informações suficientes para abrir uma.

O cruzamento de informação e a condição das fronteiras locais constituem entraves no âmbito da investigação criminal, apresentando-se como os maiores desafios na continuação da ação das forças de ordem da polícia e é, neste enquadramento, que as capacidades de *Palantir Technologies* são chamadas a atuar no fornecimento do seu software, através da negociação e estabelecimento de parcerias com o Estado.

Em termos de vantagens e desvantagens da cooperação entre agências governamentais e empresas como *Palantir Technologies*, é possível introduzir aqui algumas. Começando pelas vantagens, desvela-se que as empresas de software trazem uma proposta de valor às agências de *law enforcement* ao gerir, como já foi referido, diversos e extensos dados sensíveis através de uma plataforma singular que faça a gestão dos mesmos ao mesmo tempo que, é dado o garante da criação de um canal seguro e fiável para estas agências prosseguirem com os seus casos de investigação. De acordo com representante de *Palantir Technologies*, as palavras-chave que

refletem as vantagens da cooperação são: competência, utilidade e fiabilidade no uso destas plataformas de integração de dados (Entrevista realizada a um representante de *Palantir Technologies* 2023).

Quanto às desvantagens no que diz respeito à cooperação das agências de segurança com empresas privadas no âmbito de *policing*, que importam referir tendo em conta que a ação destas autoridades está diretamente ligada à segurança pública, englobam-se: a dependência num sistema para esta integração de dados, o que gera o risco de *vendor lock-in* (“aprisionamento” de fornecedor), isto é, é criada uma abordagem burocrática no momento em que estes clientes pretendem retirar-se destes sistemas; o custo destas plataformas representa outra desvantagem e, portanto, no momento de ponderar as alternativas, as agências refletem sobre outras possibilidades como desenvolver a sua própria plataforma no entanto, este cenário é muitas vezes mais caro do que a respetiva contratação com terceiros. Outro dos desafios que se coloca à cooperação é o facto de certos protocolos no âmbito das políticas de privacidade entre as partes poderem representar uma área cinzenta, algo que o representante distancia *Palantir Technologies* de, mas sugere que nestas parcerias torna-se necessária uma clara negociação dos termos da segurança da informação uma vez que, por ter informação sensível pertencente ao Estado, é uma questão vital que se coloca. De acordo com o representante entrevistado, *Palantir Technologies* não cria estes problemas, que, pelo contrário, apresenta soluções para os mesmos como a extensibilidade e utilização de *APIs*, através de *open data sources* (fontes que disponibilizam dados de forma acessível e gratuita ao público, normalmente sem restrições de licenciamento), que geram a possibilidade de exportar e importar dados de forma flexível.

Trata-se agora o que concerne à existência de condutas e diretrizes concretas, relativamente à questão da privacidade e do tratamento dos dados dos utilizadores do software da empresa. Isto é, procurou-se refletir na entrevista sobre a existência de comandos de censura relativamente ao tratamento desses mesmos dados dos utilizadores e, procurou-se refletir também, sobre os momentos em que existe uma cooperação complementar com terceiros para discernir se as políticas de privacidade convergem.

De acordo com o representante de *Palantir Technologies*, a empresa nunca se apodera dos dados dos seus clientes, algo que é determinado na fase de negociação das suas parcerias. Reflete-se, nesta fase, sobre o exemplo da cooperação de *Palantir Technologies* com a empresa Amazon, uma parceria estratégica. *Palantir Technologies* utiliza o Amazon *Web Services (AWS)*, plataforma de serviços de computação em nuvem que, de acordo com o representante

entrevistado de *Palantir Technologies* pode ser requerido ou não. Ou seja, *Palantir Technologies* pode requerer o recurso a este serviço de alojamento em nuvem para os seus dados a qualquer momento, mesmo em momentos de parceria com autoridades policiais, quando não está sendo utilizado um serviço próprio e seguro nas instalações destas autoridades. No entanto, existe um fosso entre as obrigações e as expectativas aquando da utilização deste tipo de servidores, ao ser apenas esperado que a empresa *Amazon* reflita na sua ação, os mesmos códigos de conduta de *Palantir Technologies*. Isto é, ao ter acesso aos mesmos dados sensíveis de *law enforcement* que *Palantir Technologies* tem, ao incorporar os seus dados, é esperado por esta última que a empresa *Amazon* proceda da mesma forma. O que leva a concluir que existe uma abertura, ainda que ínfima, para que estas obrigações não sejam cumpridas, mas que, existe um sentimento de esperança de que serão cumpridas aquando da complementação dos seus produtos com terceiros ao lidar com estas agências governamentais, o que não reflete a responsabilização e transparência desejada.

Apesar de não ser possível a divulgação dos presentes contratos entre *law enforcement* e *Palantir Technologies* é anunciado no site oficial da empresa a 26 de setembro de 2022 a informação de que o departamento de *Homeland Security* renovou o contrato com a empresa no apoio às *Homeland Security Investigations (HSI)* com a utilização do software *Investigative Case Management (ICM)*. Esta renovação de contrato tem um valor estimado de 95, 9 milhões de dólares durante um período de cinco anos (*Palantir Technologies* 2022). Tendo em atenção que as agências de *law enforcement* do Departamento de Segurança Interna dos EUA trabalham em estreita colaboração com os parceiros do ramo ao nível federal, estatal, local, e territorial de forma a compor integralmente a defesa interna da população. Estes parceiros representam a primeira linha de detenção e prevenção do país e são vitais para a segurança pública em todas as comunidades americanas (Departamento de Segurança Interna dos EUA s.d.).

É necessário, neste ponto da investigação, que haja uma ressalva relativamente ao estudo de caso aqui escolhido e as suas três instâncias principais. Ressalva, esta, que indica que os dados apresentados não foram escolhidos por corroborarem o argumento principal apresentado nesta dissertação, mas por serem os dados a que existe um maior e mais completo acesso quando estamos a determinar a envolvimento da empresa em questão com os EUA. Para além disto, as parcerias que comportam o estudo de caso representam um ponto de viragem, no que se refere à utilização e na recorrência por parte dos departamentos de *law enforcement* a um *predictive policing* e ao que autores como Sarah Brayne e Angèle Christin (2020) tratam como *intelligence* -

led policing, algo que irá ser abordado mais à frente na exploração do estudo de caso. As parcerias aqui tratadas são analisadas por ordem cronológica, isto é, a análise inicia-se com a parceria entre *Palantir Technologies* e o departamento da Polícia de Los Angeles, que começou primeiro, em 2011, em seguida a parceria com o departamento da Polícia de Nova Orleães em 2012 e, por fim, a colaboração com a agência governamental *ICE*, em 2014.

Capítulo III. Imperativos do capitalismo de vigilância na cooperação entre EUA e *Palantir Technologies*

3.1. A cooperação de *Palantir Technologies* com Departamentos da Polícia dos EUA

Os departamentos de *law enforcement* dos EUA estão em representação, neste trabalho de investigação, da figura do Estado na fusão que é sugerida no argumento principal desta dissertação. Uma fusão entre o Estado e a empresa privada analisada, *Palantir Technologies*, na forma de uma cooperação entre as partes na recolha incessante de dados.

Este capítulo inicia-se com a introdução e caracterização mais descritiva de cada parceria, fazendo ainda uma análise exploratória sobre de que forma o software de *Palantir Technologies* esteve ao serviço destas unidades de segurança em termos práticos. Segue-se, para cada segmento do estudo de caso, uma identificação sistemática dos dados utilizados⁴⁰ pelas partes, encerrando com o reconhecimento da utilização de uma vigilância massificada por parte do Estado, EUA, através de uma colaboração com a empresa, *Palantir Technologies*.

3.1.1. A cooperação de *Palantir Technologies* com o Departamento da Polícia de Los Angeles: A operação *LASER*

O departamento da polícia da cidade de Los Angeles (DPLA), na Califórnia, é o terceiro maior departamento dos EUA, antecedido pelos departamentos da cidade de Nova Iorque e Chicago. Para além disto e, acrescendo às razões já mencionadas na escolha deste estudo de caso, está a realidade de que este departamento foi dos primeiros e dos contínuos investidores na adoção de práticas baseadas na análise de dados e na integração de tecnologias que permitem a inclusão e visualização de vários conjuntos de dados, nomeadamente em cooperação com as empresas *Palantir Technologies* e *PredPol*. Cabe aqui referir ainda que, há um conjunto de fatores

⁴⁰ Entre os quais: nome, morada, características físicas, informações acerca do veículo, afiliações a gangues, registo criminal, número de telemóvel, informações sobre alvos de investigações, associados, testemunhas, informadores e terceiros bem como, publicações/fotos nas redes sociais.

que levam à aplicação de novos métodos tecnológicos para a análise de dados, salvaguardados por estas mesmas empresas quando falamos, nomeadamente, do Departamento da Polícia de Los Angeles.

Voltando à questão central para este subcapítulo, parte empírica nesta dissertação, a ligação do Departamento da Polícia de Los Angeles a *Palantir Technologies*, apresenta-se o grande fator propulsor que leva a que cada vez mais, atualmente, se integrem estas tecnologias preditivas que organizam, convergem e estruturam as diversas e variadas coleções de dados, no que diz respeito a *law enforcement*.

“Smart Policing data goes beyond traditional police information resources; it uses police intelligence as well as data on calls for service, offenses reported, arrests, and complaints that are correlated with mapped locations of various “hot spots.” Smart Policing also includes research data (e.g., offender- or location-based studies), data from external entities (e.g., hospital databases), and data from external justice agencies (e.g., probation and parole).” (Bureau of Justice Assistance 2013, 2).

Este projeto promove a integração assídua destas tecnologias que se presume que permitam a prevenção do crime, mas permitem também que novas bases de dados sejam adicionadas ao leque já existente em cada departamento. É aqui que começa a função liderante de *Palantir Technologies*, na integração e análise consistente desta acumulação de dados, bem como por parte da *PredPol* que faz a análise algorítmica do risco de acontecer novamente um crime em determinada localização (Brayne 2017, 989).

Para além de ser a terceira maior agência de *law enforcement* e líder na inteligência analítica, análise computacional sistemática de dados e estatísticas, como referido anteriormente, outra das razões para haver uma maior pressão sobre este departamento é o facto de, entre 2001 e 2009, o Departamento de Justiça dos EUA ter levado a cabo um decreto de consentimento juntamente com o DPLA. Decreto que simbolizava um acordo entre as partes para a resolução de um litígio que envolvia o departamento, decreto que era aprovado pelo tribunal. Parte destas

disputas envolviam o *Rampart Scandal*⁴¹, e o caso de brutalidade de Rodney King⁴², com encetar na década de 90. Este decreto exigia que o departamento criasse um sistema de gestão de risco dos funcionários da agência, um sistema orientado por dados, denominado TEAMS II. Ademais, era exigido ao DPLA uma maior partilha de informação entre as instituições e o assegurar de uma diretiva “data-driven decision making”⁴³ (Brayne 2017, 984).

A estes fatores, juntam-se mais dois. O facto de na legislatura do Estado da Califórnia ter passado o projeto de lei (AB 109) que transfere a responsabilidade pelo percurso dos prisioneiros recentemente libertados para os departamentos locais de *law enforcement*, na medida em que há um acompanhamento próximo e mais apertado deste grupo de indivíduos por meio da vigilância destes departamentos para que se reduza a percentagem da população prisional nos EUA. Com o somar destas questões verifica-se a rápida incorporação de novas tecnologias de integração e análise de dados neste departamento de forma que seja possível solucionar os parâmetros anteriores (Brayne 2017, 985).

Assim, apresentado o contexto essencial que abriu caminho para a integração de novos métodos analíticos junto do departamento, tem-se que, finalmente em 2011, a incorporação de *Palantir Technologies* ao DPLA. Hoje, em última análise, *Palantir Technologies* estende-se a diversos mecanismos de segurança: CIA; FBI; ICE; NSA; DHS; J.P. Morgan. Em boa verdade, foi o *Joint Regional Intelligence Center (JRIC)*, o centro de fusão de *intelligence* do Sul da Califórnia que começou por integrar a empresa *Palantir Technologies* nos seus esforços em 2009. O *JRIC* é uma parceria entre as diferentes divisões administrativas e agências públicas de segurança com objetivo de aprofundar a partilha de informação entre as mesmas de modo a detetar, deter e defenderem-se perante ameaças terroristas e outras grandes ameaças no espectro do crime (Joint Regional Intelligence Center s.d.). Dentro do DPLA existem 21 divisões e *Palantir Technologies* abrange 14 dessas áreas. Para além disso, em 2014, *Palantir Technologies* ganhou então um lugar nas Propostas do projeto AB 109, referido anteriormente, legislatura que cobre a Grande Los Angeles.

⁴¹ *Rampart Scandal*, um escândalo sobre a corrupção policial existente no departamento de Los Angeles, dentro da divisão anti-gang: *CRASH (Community Resources Against Street Hoodlums)*, para além de casos de conduta deficiente e violação de direitos humanos direcionados para a questão racial que resultou num conjunto de 140 ações judiciais contra o departamento.

⁴² Rodney King, um dos casos mediáticos de violência policial pelos quais o departamento de Los Angeles esteve indiciado, depois de ter sido agredido violentamente por um grupo de polícias, polícias que mais tarde foram acusados. Ainda assim, o veredito com 3 absolvições levou a que decorresse um distúrbio na cidade, em jeito de protesto e indignação devido à atitude policial para com minorias raciais.

⁴³ Tomada de decisão orientada por dados, no uso de ferramentas de inteligência digital para analisar fontes de dados, estruturar e organizá-las e daí gerar uma análise estatística para retirar conclusões que suportem a tomada de decisão.

Em 2011, torna-se oficial a incorporação de *Palantir Technologies* no DPLA através da integração da tecnologia disponibilizada pela empresa na conhecida Operação *LASER* (Los Angeles' *Strategic Extraction and Restoration program*). Esta operação era um dos projetos pioneiros no que toca ao uso destas tecnologias e do uso de *BigData* para realizar a análise preditiva e, pioneira no sentido que fazia uso dos dados facultados para criar um sistema de pontos avaliadores que serviam de cálculo para quantificar o risco de cada indivíduo na perpetração de um crime. Começa-se aqui por ver a transformação das práticas de vigilância e de acumulação de informação no seio de *law enforcement*, pois não é possível acompanhar nem conhecer a verdadeira retenção de informação que existe por parte destas tecnologias que estão ao serviço do Estado sem esquecer que por meio de empresas privadas, que são os principais negociadores na mesa de tomada de decisão quando se trata de dados e o acesso aos mesmos (Brayne 2017). Esta cooperação aprofundada entre o Estado e as suas unidades de segurança e as empresas privadas detentoras destas tecnologias, algoritmos e inteligência artificial é um fenómeno extraordinário que, só foi possível, pelo menos tão cedo e, de forma tão célere e aprofundada devido ao excecionalismo de vigilância permitido com o pós-11 de setembro sugerido também por Shoshana Zuboff (2019).

A Operação *LASER* foi financiada pela *Smart Policing Initiative*, isto é, por fundos do governo federal, e englobava não só o método de *actuarial justice*, termo anteriormente referido, ligada à gestão e cálculo do risco, conhecido por *risk-management deployment*, mas também através de táticas e estratégias de *stop-and-frisk* (parar e revistar) e *hotspot policing*.

O consultor do departamento Craig Uchida foi o promotor das estratégias e figura importante na criação desta operação que resultava do incentivo do Estado através desses fundos, mas, vinha também como consequência da adoção de novas tecnologias e do estado de alerta das unidades de segurança que transformavam a sua ação na chamada *dragnet surveillance*. *Dragnet surveillance* é então uma posição e um estado de alerta permanente das forças policiais que engloba um conjunto de estratégias no terreno de modo a intersectar não só pessoas sob suspeita mas que permitam alargar a informação sobre o maior número de civis possível, ou seja, de modo a estabelecer uma rede de correlações entre os vários dados que, neste estudo de caso, são estruturados, identificados e notificados através da tecnologia disponibilizada por *Palantir Technologies*, alargando assim a supervisão sobre a população doméstica, monopolizando a informação através do acesso aos dados de várias instituições de diferentes domínios sobre

aqueles que não sabem que estão sobre a alçada vige de *law enforcement* (Brayne 2020; Brayne 2017, 979).

Assim, juntamente com a Operação *LASER* foi criado o *Crime Intelligence Detail (CID)*, que consistia no agrupamento de três oficiais e um analista de crimes que procediam à contextualização dos dados para identificar os crimes, as pessoas e o local (Information Technology Bureau Los Angeles Police Department, e Dr. Craig D. Uchida 2014, 1). Ainda dentro deste projeto existiam duas alternativas na identificação do crime e dos possíveis infratores, uma estratégia *place-based*, ou seja, com a análise dos dados e com o processamento do algoritmo tentavam identificar as principais zonas problemáticas, as chamadas *LASER Zones*, que por ventura determinariam a patrulha regular e acentuada nessas zonas, isto é, nas áreas passíveis de uma maior percentagem de crime, sendo que se o crime tivesse ocorrido nessa zona toda a área envolvente estaria em alerta para o DPLA devido ao risco calculado de crimes subsequentes, este método foi facilitado pelo software da empresa *PredPol*, mais tarde, em 2012 (Brayne 2017, 989; Mark Harris 2017).

Uma outra estratégia consistia no modelo *offender-based*, isto é, o foco estava na busca pelo infrator, por suspeitos, e pessoas ligadas ao crime. Esta estratégia, de relevância para o estudo de caso, uma vez que foi com esta estratégia que *Palantir Technologies* obteve o papel fundamental no seio do departamento, que levou a um trabalho em conjunto entre o departamento e a empresa. Este modelo foi implantado primeiramente numa área com um histórico problemático de crime, *Newton Division*, em que seriam identificados e encaminhados recursos para esta área, visando detetar os indivíduos de maior risco, classificados no programa de *Palantir Technologies* através de uma escala gerada pelo *CID* (Harris 2017).

Esta divisão, *CID*, propõe-se a recolher informação, *intelligence*, através de várias frentes de interseção policial, desde patrulhas, a cartões de entrevistas no terreno, isto é, contacto direto com a polícia, até registos de sinalizações no trânsito, relatórios de crimes e detenções, formulários de libertação e quaisquer registos de antecedentes criminais. A partir desta fase é criada uma lista de *chronic offenders*, com uma escala classificatória dos indivíduos, a quem é atribuído um “valor” em pontos a cada pessoa e uma classificação numérica de acordo com esse valor. Os pontos dados a indivíduos com certos tipos de infrações tiveram alterações ao longo do percurso da Operação *LASER*, sendo que a última atualização da escala mantinha o seguinte: 5 pontos por cada crime violento no seu registo criminal; 5 pontos por associação a gangues; 5 pontos por cada incidente que envolva qualquer tipo de arma, nos últimos dois anos; 5 pontos se estivessem em

liberdade condicional ou em regime de liberdade provisória e, 1 ponto por cada contacto de qualidade com a polícia, nos últimos dois anos (Office of the Inspector General 2019).

Através do *Software as a Service (SaaS)* proclamado pela empresa é possível para o DPLA usar dos produtos e do *software* de *Palantir Technologies*, de modo que este contexto de *predictive policing* e combate ao crime seja possível (Palantir Technologies 2020). Fazendo uso do sistema operativo Gotham proporcionado por *Palantir Technologies* torna-se mais fácil para o DPLA de organizar informação, criar alertas de ligação entre os dados e apresentá-los de forma célere, pois antes de *Palantir Technologies* já existiam os chamados *Chronic Violent Crime Offender Bulletins* que reúnem as informações acima descritas recolhidas pelo *CID*, no entanto, o que demorava tempo a recolher e a procurar possíveis ligações entre dados, demorava agora apenas alguns minutos devido à amplitude excecional dos produtos da *Palantir Technologies*.

De notar que através da correlação de informação entre as bases do DPLA, *CID* e outras bases institucionais junto com *Palantir Technologies* é possível este insólito agregar de informação, que permite que o *predictive policing* entre em ação vis-à-vis a ameaça global do terrorismo e o combate ao crime numa visão mais exígua, ao nível local. É, então, na aposta em *Palantir Technologies* que é possível perceber o desenvolvimento de departamentos de *law enforcement* como o de Los Angeles, com o recurso a fundos governamentais, na adaptação de uma posição centrada no uso de tecnologias avançadas para responder às novas exigências de um *policing* orientado por dados, voltado para o uso do algoritmo, no combate ao crime. No entanto, é importante salientar que para este trabalho com o departamento de Los Angeles, *Palantir Technologies* apenas menciona o seu apoio às autoridades enquanto potenciadora de integração de dados e da organização e visualização de dados estruturados e não estruturados, ao invés de um reconhecimento de uma análise preditiva.

Palantir Technologies, que tem uma rede de acesso a informação que ultrapassa a compreensão da sociedade civil pois sendo uma empresa privada com sede nos EUA indica uma barreira no acesso total de informação quanto aos recursos e fontes a que *Palantir Technologies* tem alcance, uma vez que no sistema jurídico norte-americano não existe tanta regulamentação em relação aos dados como, por exemplo, em comparação, com a número 1 neste ramo, a União Europeia e , por isso, tal como simplifica Frank Pasquale, para além de informação mais atualizada:

“(…), é simplesmente mais fácil para as autoridades adquirirem dados recolhidos pelo setor privado do que confiar em dados internos, uma vez que

existem menos proteções constitucionais, requisitos para reportar, e menor controlo sobre os recursos de vigilância e recolha de dados do setor privado.”⁴⁴
(Frank Pasquale citado por Brayne 2017, 995).

De acordo com Sarah Brayne, há ainda uma importante questão a adicionar, ao refletir os vários níveis de informação que eram facilmente proporcionados e integrados no sistema de *Palantir Technologies* na assessoria ao departamento. A informação gerada pelo *CID*, acima mencionada, era automaticamente integrada e complementada no programa de *Palantir Technologies*, constituindo um papel vital aqui os cartões de entrevistas no terreno, ou os chamados *field interview cards (FIs)*, que representam uma fonte promissora de *intelligence*.

Os *FIs* incluíam informações pessoais como nome, morada, número de telemóvel, características físicas, informações acerca do veículo, afiliações a gangues e histórico criminal, para além de que dava espaço para o agente anotar qualquer tipo de informação adicional. Mais tarde, e através dos documentos processados por uma comunidade organizada e enraizada contra a vigilância da população em Los Angeles, *Stop LAPD Spying Coalition*, foi possível atualizar a informação que era integrada no programa de *Palantir Technologies* através destes *FIs*: a partir de 2015, o departamento começou a reunir informações extraordinárias, sob a forma destes *field interview cards*, acerca das redes sociais, os números de segurança social e ainda, os endereços de email de cada indivíduo que abordavam. Assim, *Palantir Technologies* conseguia construir o mapa do percurso (ver **Anexo II**) de cada indivíduo ligando estas informações e associando a lista de amigos nas redes sociais bem como, o reconhecimento de pessoas em fotos nessas mesmas levando a que, se necessário, mais tarde, estas associações eram apresentadas na forma de ações judiciais ligadas a conspiração e a reconhecimento de gangues (Stop LAPD Spying Coalition 2021, 9). Estes *FIs* são uma parte crucial e uma ferramenta indispensável para a construção de *intelligence* para proceder com as investigações criminais, por esse motivo foram das primeiras fontes a serem integradas na plataforma de *Palantir Technologies* para esse mesmo efeito. Para além disso, uma vez no sistema esta fonte de informação é marcada com a hora, data e coordenadas geográficas, o que se revela fundamental para quando existe um alerta derivado da correlação destas diferentes fontes de informação, isto é, cria-se um aglomerado de informações diversas e, a sua soma pode posteriormente tornar-se a peça chave para construir o que é necessário para levar a cabo a ação e as investigações do departamento (Brayne 2017, 987).

⁴⁴ Tradução livre de: (...), it is simply easier for law enforcement to purchase privately collected data than to rely on in-house data because there are fewer constitutional protections, reporting requirements, and appellate checks on private sector surveillance and data collection.

Com os avanços da tecnologia ao longo dos anos, já no momento da operação *LASER* (2011), é possível argumentar que este método de recolha de *intelligence*, os *FIs*, seriam antiquados dado os métodos existentes. Seria possível até, atribuir-lhes um carácter anacrónico perante o presente, no entanto, existe uma explicação basilar para a sua recorrente utilização, sendo esta, o facto de que a polícia não necessita de adquirir um mandado pelo tribunal para realizar estes contactos e este preenchimento de *FIs*, que como já foi demonstrado revelam informações pertinentes (Brayne 2017).

Ademais, à polícia, de acordo com a Quarta Emenda à Constituição dos Estados Unidos, não lhe era permitido realizar buscas e apreensões na falta de causa provável, no entanto, foi sendo marcado um caminho em direção ao que já foi mencionado de recolha de *intelligence* no seio de *law enforcement* ainda antes da expansão de *BigData* (Brayne 2017).

Através da introdução de certas decisões do Supremo Tribunal que tornavam a investigação e o trabalho destes departamentos mais simplificado, com a construção de um cenário de crime com a acumulação de *intelligence*, que contribuía para reunir as condições que justificavam o mandado de detenção/busca e, contribuía em última análise aos olhos do departamento para satisfazer o objetivo cardinal de um decréscimo na taxa de criminalidade. Como exemplo destas decisões: *Terry v. Ohio* 392 U.S. 1 (1968)⁴⁵, que instituiu a proliferação de contactos policiais baseados na suspeita razoável, a qual tem de ser baseada em factos específicos e articuláveis e não apenas em palpites dos agentes, no entanto deixa de ser necessária a causa provável. Assim, voltando à questão principal, para abordar uma pessoa e estabelecer esse contacto, gerando nova informação e colocando-a no sistema de *Palantir Technologies*, o agente apenas necessita dos *FIs*, que perfazem uma abordagem consensual. Após esse momento, são integrados no sistema somando pontos à pessoa de interesse. Mais tarde, esta colaboração com o sistema operativo da empresa vai ligar os *FIs* a outras informações já registadas anteriormente, provenientes de outras fontes e bases institucionais a que o Estado lhe deu acesso por estar em colaboração com o departamento num período de crise, que vão servir para montar o palco para que aqui assim, já haja uma causa provável e seja possível emitir um mandado de detenção/busca.

No entanto, com a decisão supracitada tornava-se mais fácil para o departamento levar alguém à justiça com a concessão da estratégia parar e revistar, *stop and frisk* na base de uma

⁴⁵ Uma decisão e um marco na história do Supremo Tribunal de Justiça dos EUA, que estabelece um precedente nas práticas das autoridades de *law enforcement* ao reiterar que a prática "*Stop and Frisk*" se torna constitucional para a polícia norte-americana. No sentido em que, se torna possível parar e revistar uma pessoa sob as condições de suspeita razoável por posse de arma ou da ocorrência de um crime (*Terry v. Ohio*, 392 U.S. 1 (1968)).

suspeita razoável, que é obtida agora de forma regular e simplificada devido ao agregar de dados e correlação de informação contextualizada que *Palantir Technologies* oferece. *Palantir Technologies* obtém facilmente a *intelligence* necessária acerca de uma pessoa com o acesso instantâneo a este núcleo de dados que lhe é atribuído com o consentimento do Estado, não só com a ausência de proteções constitucionais, mas também porque este acesso a informação se dá de forma invisível aos olhos alheios. Esta ação compressiva que cinge a população no seu quotidiano é derivada de um estado de guarnição e de uma tomada de decisão voltada para o algoritmo, pela promessa de uma maior eficácia e certeza que passa pela inclusão do maior número de pessoas e o máximo de dados no novo complexo de *policing* (Brayne 2017, 987).

De ressaltar que, da mesma forma que uma pessoa com uma classificação alta era passível de ser abordada e ter um contacto com a polícia, esse mesmo contacto somava um ponto à sua classificação no ranking do departamento, gerando uma bola de neve no gerar da lista de *chronic offenders* e, nas suas respetivas classificações (Brayne 2017, 987). Mais tarde, acaba por ter um efeito de *spillover*, pois qualquer pessoa é passível de ter um contacto policial e ser integrada no sistema de *Palantir Technologies* para futuras investigações com a correlação de dados. Com isto, foi possível perceber na investigação, a transformação das práticas policiais para o pináculo da vigilância ao proceder com o objetivo de integrar o máximo de pessoas no sistema, o que também conseguimos perceber através do **Anexo II**. Isto é, muitas vezes uma pessoa sem qualquer contacto policial anterior já estava dentro do sistema de *Palantir Technologies*, através por exemplo da associação na lista de amigos nas redes sociais, às quais *Palantir Technologies* recorre para a sua análise sem que a sua atividade seja restringida por proteções jurídicas.

Esta componente na transformação das práticas policiais em direção à vigilância em massa é denominada de *Lower Database Inclusion Thresholds*, pela autora Sarah Brayne (2017), na medida em que são incluídas pessoas sem contacto policial anterior, por meio de diagramas de redes de contacto (ver **Anexo II**). Isto é, indivíduos ligados de alguma forma à pessoa de interesse para a polícia, estão inseridas no radar vigilante de *Palantir Technologies* que encaixa todas as ligações e referências à pessoa de interesse e as suas conexões. A somar a isto agrega-se ao facto de serem monitorizadas pessoas fora do alcance policial uma potencialidade de *Palantir Technologies* de alertar em tempo real o departamento se estas redes de contactos da pessoa de interesse estabelecem contactos com a polícia ou outras agências governamentais, aqui, podemos ver o exemplo prático da missão declarada levada a cabo por *Palantir Technologies*:

Software *as a Service* (Palantir Technologies 2020). Através da incorporação do maior número de indivíduos no sistema assistimos a uma mais-valia que interseja os dois atores mais importantes neste palco da vigilância, o Estado e a empresa, os objetivos são diferentes, no entanto, o resultado propõe-se a ser o mesmo, o que demonstra a causa válida de uma preocupação através da contínua investigação no que diz respeito à vigilância massificada da população, nos termos de quem e com o conhecimento de quem se procede esta vigilância. Por consequência, este credo é interpretado na literatura com uma nova designação: *Surveillance as a Service* (Iliadis e Acker 2022, 338).

A somar a esta *Lower Database Inclusion Thresholds* temos outro aspeto controverso em relação a estas capacidades que os departamentos de *law enforcement* adquirem por meio de empresas de software, os *ALPRs* (*The Automatic License Plate Reader* – Leitor Automático de Matrículas). Estes *ALPRs* são detentores de um mecanismo acionável que inclui na sua base de dados um número maior de indivíduos pela sua capacidade de leitura de matrículas que não são exatamente procuradas pela polícia. Esta ferramenta faz parte das estratégias de *dragnet surveillance*, referida anteriormente, que através de câmaras nos carros da polícia ou em postos estáticos nas ruas tiram uma foto da matrícula e outra do carro, posteriormente através das capacidades da empresa, no caso *Palantir Technologies*, é atribuído a estas fotos a hora, data e as suas respetivas coordenadas. Estes dispositivos servem à polícia para a construção do mapa da distribuição de veículos nas cidades e, noutras circunstâncias, pode contribuir para identificar os padrões de deslocação de um indivíduo de interesse (Brayne 2017, 992). *ThunderBird* é o nome que designa o sistema de *Palantir Technologies* que circunscreve este *ALPRs*:

“A integração de matrículas na plataforma através de *ThunderBird* acrescenta novas capacidades: a monitorização de comportamentos ao longo do tempo e a capacidade de localizar um indivíduo no espaço. Estamos perante uma amplificação radical das capacidades de vigilância, ao facilitar a identificação e o interrogatório de indivíduos em grande escala. Desta forma, *Gotham* proporciona uma expansão significativa no âmbito da análise de dados, ao mesmo tempo que facilita a sua utilização sem dificuldade, isto é, uma economização na regulação dos indivíduos.” (Munn s.d., 12)⁴⁶.

⁴⁶ Tradução livre de: Integrating license-plate data into this platform via Thunderbird adds new capabilities: the tracking of behaviors over time and the ability to locate a subject in space. This is a radical amplification of surveillance capabilities—facilitating the targeting and interrogation of subjects

Palantir Technologies proporciona aos departamentos de *law enforcement* uma aproximação na totalização de informação acerca de todos os indivíduos, através do suporte do seu software que organiza e visualiza de forma uniformizada dados estruturados e não-estruturados de várias fontes e base de dados, com a marcação destes dados no sistema com um género de etiqueta virtual com as coordenadas, que são apresentadas temporalmente e espacialmente, o que permite aos agentes visualizar os dados em contexto e formular novas ligações (Brayne 2017, 994). O sistema operativo da empresa complementa com a informação necessária às investigações da polícia ao fazer o cruzamento de dados entre as fontes a que tem acesso, em colaboração com o departamento que tem por outro lado, permissão no acesso a dados de outros departamentos e de outras agências governamentais. Isto é, na necessidade dos departamentos de atingir resultados e adaptarem-se às novas tecnologias preditivas leva a que exista uma fusão consensual com empresas privadas de software, como *Palantir Technologies*, no que diz respeito ao cruzamento de dados que se multiplicam àqueles que a empresa já tem acesso por meio de um sistema neoliberal característico aos EUA, em que as restrições constitucionais às empresas são irrelevantes face às suas capacidades presentes e face às que existem perante o setor governamental, em comparação (Electronic Frontier Foundation s.d.).

De forma a proceder à consolidação da análise desta parceria, importa refletir sobre um último aspeto que traz à discussão uma perspetiva inovadora, que se trata do facto dos indivíduos deterem uma “pegada digital”. Tudo o que fazem no decorrer das suas vidas, ao nível social, profissional, medicinal, institucional passa por um fluxo digital, o qual hoje em dia, não é possível contrariar, o que leva a que exista nos termos de *BigData*, um género de *data double* (duplicado digital) dos indivíduos e das suas vidas, às quais as agências governamentais têm acesso e, ainda mais, as empresas privadas. Assim, libertando uma impressão digital, os indivíduos dão espaço para que estas entidades façam as suas reflexões e conexões com base nestes *data doubles*, podendo a partir desses, abordar e classificar os indivíduos com base nas suas reflexões na análise destes dados, que acreditam traduzir-se aproximadamente à realidade dos indivíduos. Ou seja, ao ser assegurada a incorporação de informações diversas sobre os indivíduos ao percorrer diversas bases de dados, para além das bases dados de *law enforcement*, isto é que nada têm a ver com justiça criminal, por exemplo a integração e aquisição de informações por meio de redes sociais, enquadra um novo fenómeno, ao qual Sarah Brayne (2017) designa de *function creep* - quando

on massive scales. Gotham thus provides both a significant expansion in the scope of data analysis while simultaneously facilitating an effortlessness in their use—an economization of regulation.

os dados são inicialmente recolhidos para um propósito mas são também utilizados para outros fins, o que ajuda substancialmente a polícia com o acesso a estes dados que não serviam o propósito de serem usados perante a justiça criminal anteriormente. Existe, no seio de *law enforcement*, um imperativo, *Institutional Data Imperative*, ter uma representação da população em massa através de dados, *data doubles* de toda a população (Brayne 2017, 993-994).

Até aqui, seria possível tecer algumas reflexões importantes como o facto de haver uma invisibilidade nesta ação de *law enforcement* intermediada pelas empresas como *Palantir Technologies*, na acumulação de informação e uso da mesma sobre civis que não estariam sob alerta anteriormente. Hoje, é possível perceber o carácter atrativo que a acumulação de informação sobre um maior número de pessoas tem, informação distribuída por outros domínios da vida social (Harris 2017). Esta acumulação ou capitalização de informação, como designaria Shoshana Zuboff, permite sob forma disfarçada uma triagem social da população e uma classificação através da referida quantificação do risco, por meio do mencionado fenómeno de *function creep*, triagem que permite classificar os indivíduos na escala de alto ou baixo risco quando falamos de cometer crimes, ou de serem suspeitos de atividade terrorista como é o exemplo nesta instância do estudo de caso. No entanto, esta classificação dos indivíduos pode ser alargada a vários domínios da vida em sociedade como a concessão de um empréstimo, de seguros, entre outros, devido a uma partilha de informação entre instituições. Há uma aproximação ao sistema de crédito social da China (Zuboff 2019)

Finalmente, é possível concluir com reflexões acerca da avaliação sobre a eficácia desta parceria quanto à narrativa proposta de diminuir a taxa de criminalidade.

A Operação *LASER* foi cessada de forma integral em abril de 2019, mas foi feita uma revisão dos vários parâmetros e de modo geral acerca da sua eficácia no combate ao crime. Esta revisão foi feita pelo *Office of the Inspector General (OIG)*, em 2019. Aquando desta revisão foram apurados alguns problemas acrescidos a esta Operação, para além de que os documentos fornecidos ao *OIG* foram escassos e muito limitados quanto à descrição das várias estratégias levadas a cabo com o *Chronic Offender Program*, o que permitiu à Comissão pôr em causa a consistência e legitimação desta Operação. Assim, foi identificado pelo *OIG* uma discrepância na utilização deste programa na medida em que, em certas áreas eram utilizados certos elementos do mesmo que se focaram noutros tipos de crimes que não os crimes mais violentos, o que não permitia fazer um estudo na correlação dos efeitos desse programa no seu todo nestas áreas, relativamente às taxas de crimes violentos. A somar a isto, tem-se ainda que nestas variações se

refletem problemas quanto ao controlo e supervisão centralizada do departamento quanto à aplicação do programa nas áreas designadas. Os boletins mencionados acima sobre infratores crónicos tinham diferentes modelos para as várias áreas e, alguns até tinham sido alterados face aos utilizados anteriormente, o que dificultou a apreciação do programa e, consequentemente, fazer uma análise da sua responsabilização e controlo (Office of the Inspector General 2019). Adicionalmente, um outro aspeto não só apontado por esta comissão, mas também pela comunidade, mais especificamente, pela já referida *Stop LAPD Spying Coalition*, é a entendida perseguição racial. No caso da comissão apenas foi referido que de modo geral a composição racial/étnica dos infratores crónicos aproxima-se da composição dos detidos por crimes violentos, os quais se traduzem maioritariamente por hispânicos/latinos e negros/africano-americanos. Nas ações judiciais e queixas da comunidade envolvida levaram a que na alçada do *California Public Records Act (CPRA)* fossem disponibilizadas informações que revelavam o impacto do preconceito nestas áreas e a resistência de uma cultura de discriminação:

“Em 2019, recorremos a uma ação judicial que forçou a divulgação das listas das pessoas visadas pelo departamento da polícia de Los Angeles. A nossa análise destas listas revelou que quase metade das pessoas visadas são negras (ainda que apenas constituam 9% da população da cidade), (...).” (Stop LAPD Spying Coalition 2021, 15)⁴⁷.

O encerramento desta Operação foi então, fruto de uma avaliação pelo *OIG* que concluiu a falta de dados pertinentes ao estudo da eficácia do *Chronic Offender Program*, facilitado por *Palantir Technologies*, constituindo um obstáculo central nessa avaliação. Assim, o que começou com o objetivo de proporcionar ao departamento maior eficiência no combate ao crime e na ajuda ao combate ao terrorismo, acrescentando à necessidade de *accountability* (responsabilidade por) do departamento devido ao decreto referido no início desta análise resultou, contudo, numa ausência de evidências que demonstrassem eficácia no combate à criminalidade violenta. No campo da *accountability* provou-se um desvio dos objetivos pelas diferentes áreas em que o programa foi aplicado para além de que, o impacto do preconceito sentiu-se ainda assim na comunidade. Deste modo, estas ilações contribuíram para que se inferisse que estas sinergias entre o departamento e *Palantir Technologies* não tiveram os objetivos cumpridos, antes pelo contrário, tanto o *OIG*,

⁴⁷ Tradução livre de: In 2019, a lawsuit we filed forced the release of lists of the people who LAPD targeted. Our analysis of these lists revealed that nearly half the people targeted are Black (even though Black people are 9% of the city's population), (...).

como a comunidade visada interpretou esta cooperação apenas como uma nova forma viabilizada de vigiar de perto os civis colocando em risco a sua privacidade e segurança, na medida em que havia uma certa probabilidade do sistema identificar a pessoa errada e, também observava-se, em algumas áreas, a utilização do método de *deterrence of crime* (dissuasão da criminalidade) com o envio de cartas (ver **Anexo III**) aos infratores identificados no sistema, prosseguindo com uma estratégia de intimação na promessa de uma escolta ativa da vida da população (Office of the Inspector General 2019).

Em virtude de continuar com esta lógica pró-ativa de vigilância, devido ao incentivo que existe em departamentos como o de Los Angeles, com a atribuição de fundos do Estado que financiam estas cooperações congêneres com empresas privadas de software como *Palantir Technologies*, verificou-se uma iniciativa por parte do departamento em encontrar uma substituição válida à Operação *LASER*. Verifica-se esta prontidão no discurso do Chefe da Polícia do departamento, Michel R. Moore, quando anuncia o novo projeto: “Como parte do nosso esforço contínuo para melhorar o Departamento e o serviço que prestamos, continuaremos a implementar sistemas que medem os resultados, fomentam a eficiência, e asseguram a transparência” (Los Angeles Police Department 2020)⁴⁸, denominado por *Data-Informed Community-Focused Policing (DICFP)*. Este projeto não deixa de incluir *Palantir Technologies* nas muitas ferramentas de análise do departamento, no entanto agora o foco vai para os *Records Management System (RMS)*. Esta iniciativa é encarada pela comunidade visada como uma reformulação dos projetos anteriores, mas agora com um novo enquadramento, um eufemismo da tática de *predictive policing* (Stop LAPD Spying Coalition 2021).

Assisti-se a um enraizamento de uma economia política de vigilância que se mostra pró-ativa no combate ao crime, mas, no entanto, acaba por ficar pela teoria e verifica-se apenas um olhar voltado para uma maior captura de dados da população como forma de manter os apoios do Estado. A fusão entre o interesse privado e a necessidade de um departamento causa problemas ao nível da sociedade, na medida em que existe a percepção de uma diminuição da segurança ligada à falta de privacidade causada pelo imperativo do Estado, o qual se reflete numa elevação e aumento da capacidade vigilante do mesmo, ainda que ao nível da população doméstica. Vai ser possível refletir estas questões na análise das parcerias posteriores, que

⁴⁸Tradução livre de: As part of our ongoing effort to improve the Department and the service we provide, we will continue to implement systems that measure results, improve efficiency, and provide overall accountability.

espelham este novo complexo Estado-setor privado que transforma a detenção de *BigData* num cálice sagrado revelador da tutela de poder.

3.2.2. A cooperação de *Palantir Technologies* com o Departamento da Polícia de Nova Orleães

A fusão referida entre o interesse privado e a necessidade de um departamento em dar respostas, no caso do DPLA, também se verifica noutra instância deste estudo de caso, no Departamento da Polícia de Nova Orleães (DPNO).

A parceria de Nova Orleães com *Palantir Technologies* é assinada e trazida ao conhecimento da sociedade civil após a sua parceria com o Departamento da Polícia de Los Angeles.

Esta parceria entre o departamento da polícia de Nova Orleães e *Palantir Technologies* é lembrada nesta dissertação em virtude da ilustração neste estudo de caso da referida fusão entre as partes num espaço em que vigora uma economia digital e uma busca pela certeza, alcançada pela vigilância em massa. A escolha deste departamento deve-se ao maior acesso a dados relativamente a outras parcerias verificadas e, também, por trazer novas perceções para a investigação, para além de integrar parte do *illustrative case study* aqui representado. A juntar a estas questões tem-se que esta cidade foi já considerada a capital de homicídios nos Estados Unidos⁴⁹ e continua a destacar-se por razões ligadas à percentagem de crime da cidade.

Em linha com a parceria de *Palantir Technologies* com o departamento de Los Angeles verifica-se que todo este contexto de novas tecnologias preditivas aplicadas a *law enforcement* se dá no seguimento, como já foi referido, de uma diretiva aplicada pelo *Homeland Security Act*. Esta diretiva, juntamente com a aplicação de fundos do Estado a estas agências, na ótica de um maior apoio na linha da frente ao combate ao terrorismo trouxe aos departamentos um estatuto que lhes permite atuar numa capacidade de nível federal e, é-lhes delegado numa primeira fase a total decisão sobre a forma como estas tecnologias emergentes são aplicadas ao seu departamento e, em que medida são utilizadas. Para além desta diretiva que se prolonga no tempo, a celeridade com que verificamos a integração destas tecnologias deve-se também à constatação de uma conduta por parte destes departamentos da polícia nos EUA que reflete valores discriminatórios,

⁴⁹“Na altura (1994), Nova Orleães tinha a taxa de homicídios mais elevada de todas as cidades do país.” (Goldberg 2015). Tradução livre de: At the time, New Orleans had the highest murder rate of any city in the country.

ligados também ao preconceito racial, o uso excessivo da força e, muitas vezes, um policiamento inconstitucional. Isto é, a integração destas reflete também a convicção de que irão solucionar estes problemas ligados à conduta dos próprios departamentos. Estas soluções designadas inteligentes são acolhidas numa teoria de resolução de problemas, e numa percepção de que são soluções modernas e proficientes, além de futuristas, percebendo assim o caráter atrativo das mesmas para as partes (Ferguson 2017).

A teoria no mote inscrito nas ações dos departamentos da polícia traduz-se igualmente no seu objetivo principal: assegurar a segurança e saúde públicas. No entanto, quando na prática o que se constata é uma conduta inconstitucional e discriminatória que paradoxalmente limita a garantia da segurança e saúde públicas encontramos uma dicotomia desconfortante para a população, a teoria versus a prática na ação e cumprimento dos objetivos por parte de *law enforcement* (ver **Tabela 1**), nos EUA.

Esta conduta é inspecionada pelo Departamento de Justiça dos EUA, apesar de que a coordenação destas agências é feita pelo *The Office for State and Local Law Enforcement (OSLLE)*. Tal como se verificou com o departamento de Los Angeles, o Departamento de Justiça dos EUA, juntamente com a cidade de Nova Orleães chegou a uma decisão, com a emissão de um decreto de consentimento em 2013 com a promessa de uma reforma nas práticas policiais do departamento da polícia. Para a chegada deste decreto, o departamento foi alvo de uma avaliação ponderada pelo Departamento de Justiça dos EUA, reaberta em 2010 que registou os procedimentos do departamento no período que se estendia de 2005 a 2011. Tal como referido anteriormente, esta avaliação demonstrava o paradoxo identificado:

“O DPNO é, já há muito tempo, uma agência problemática. Os elementos básicos de um policiamento eficaz - políticas claras, formação, responsabilização, e a confiança dos cidadãos - estão ausentes há anos. Com demasiada frequência, os agentes demonstram uma falta de respeito pelos direitos civis e pela dignidade da população de *New Orleans* (...). À medida que violações sistemáticas dos direitos civis rompem com a confiança da população, o policiamento torna-se mais difícil, menos seguro e menos eficaz, e a criminalidade aumenta.” (Departamento de Justiça dos EUA 2011)⁵⁰

⁵⁰Tradução livre de: The NOPD has long been a troubled agency. Basic elements of effective policing - clear policies, training, accountability, and confidence of the citizenry - have been absent for years. Far too often, officers show a lack of respect for the civil rights and dignity of the people of New Orleans (...). As systematic violations of civil rights erode public confidence, policing becomes more difficult, less safe, and less effective, and crime increases.

Os padrões e práticas identificadas nesta avaliação variam entre: o uso excessivo de força; paragens, revistas e detenções que violam a Quarta Emenda à Constituição dos Estados Unidos e, um policiamento discriminatório (Departamento de Justiça dos EUA 2011). Com o decreto de consentimento de 2013, a promessa estava em reformas sistêmicas e estruturais, com relatórios anuais que provassem o cumprimento destas e a complacência do departamento com as novas práticas (United States District Court Eastern District of Louisiana 2013). Nestes documentos, na avaliação do departamento em 2011 e no decreto de consentimento de 2013, regista-se o efetivo incentivo e impulso à integração de tecnologias às quais são dados créditos quanto à transparência na tomada de decisão, a eficácia dos produtos e, a questão da *accountability*, isto é, aquando da integração e promoção destas tecnologias de integração e visualização de dados, é atrelada a crença de que estas irão resolver os problemas do departamento por garantirem, na teoria, o cumprimento desses créditos.

Num primeiro momento e, após a análise feita na revisão da bibliografia no início desta dissertação é possível afirmar, que é em momentos de crise onde se verifica um estado de alerta pelos governos em que a ação imediata passa pelo decreto de medidas extraordinárias. Sendo que essas mesmas medidas se sobrepõem a leis e direitos já estabelecidos, numa narrativa de que o mais importante, naquele momento, é ultrapassar a crise securitária no país mesmo que algumas medidas não sejam particularmente descritas como democráticas. Verificou-se isso com o 11 de Setembro, com um conjunto de medidas e leis que expandem a capacidade vigilante do Estado e, vimos também, com o exemplo da pandemia do Covid-19, em que a liberdade de movimentação da população é posta em causa e, a vigilância das massas emerge na arena disruptiva através duma parceria com empresas privadas em que a população é acompanhada nas 24 horas do seu dia através dos dispositivos móveis, no mote de que só assim é possível combater a propagação da epidemia. A autora Carissa Véliz reflete sobre esta urgência:

“Durante as crises, as decisões são tomadas sem a devida consideração dos prós, dos contras, dos indícios e das alternativas. Sempre que há a menor resistência a uma medida extrema proposta, o apelo à “salvação das vidas” silencia as vozes discordantes (...). As liberdades civis são sacrificadas injustificadamente, sem as garantias adequadas de que sejam repostas depois da crise. Medidas extraordinárias tomadas no auge do pânico tendem a manter-se muito depois de a emergência ter passado.” (Véliz 2022).

A parceria com o DPNO representa mais um exemplo de um momento de crise em que se recorrem a medidas extraordinárias, com a coordenação da ação do departamento junto de empresas de software como *Palantir Technologies*. Em 2013, Nova Orleães registava a sexta taxa mais elevada de homicídios dos Estados Unidos e, perante este cenário turbulento, o presidente Mitch Landrieu para além do pedido de avaliação do departamento em 2011, optou pela criação de um programa que tinha em vista a transformação da cidade em termos de criminalidade para além de um apoio à sua população com a aprovação de programas direcionados às infraestruturas e serviços fulcrais para a cidade de *New Orleans* (Winston 2018).

O programa designado *NOLA For Life*, aprovado em 2013, tinha como objetivo estabelecer um conjunto de estratégias que permitissem a redução da taxa de homicídios e a violência na cidade, de forma geral. Com o direcionamento para a violência juvenil, este programa tinha o apoio do *National Forum on Youth Violence Prevention*, um fórum sem fins lucrativos que reúne diversos setores e ramos da cidade, em que o objetivo decretado no documento oficial do programa é melhorar a segurança entre os jovens e interceder sobre os fatores de risco e proteção da violência juvenil (The City of New Orleans Health Department 2013). Mais uma vez é entendido, também para este departamento de *law enforcement*, que a solução está na adoção de estratégias “*data-driven*”, isto é, agências governamentais locais a usufruir de produtos de empresas de software para ajudar no processo de tomada de decisão no que diz respeito à forma como estas comunidades, estas pessoas, vão ser policiadas no dia-a-dia: “Além disso, o *PLAYbook* enfatiza as ferramentas da saúde pública: foco na prevenção, estratégias baseadas em dados, colaboração, e uma escala de ação ao nível da população.”⁵¹ (The City of New Orleans Health Department 2013, 10). Assim sendo, é com base nas técnicas apresentadas pelas empresas que os departamentos formam parcerias com as mesmas numa interpretação persuadida de que estas capacidades se vão aplicar à resolução de problemas nas cidades.

Palantir Technologies, tal como outras neste ramo, uma empresa que iniciou a sua atividade voltada para a atividade do exército e a vertente militar é requerida no âmbito do *policing* destes departamentos locais. A dúvida que se coloca é como tais técnicas requeridas pelo militar chegam ao perímetro destas unidades de segurança, ponto que a autora Sarah Brayne faz questão de salientar por ser uma prática comum:

⁵¹ Tradução livre de: In addition, the *PLAYbook* emphasizes the tools of public health: a focus on prevention, data-driven strategies, collaboration, and a population-level scale for action.

“Do lado dos representantes de *software* é demonstrada a utilização das suas plataformas num contexto não-policial, normalmente militar e, de seguida, é questionado às autoridades policiais locais se haveria interesse numa aplicação semelhante ao seu contexto. Ou seja, em vez de serem preenchidas lacunas analíticas ou vazios técnicos identificados pelas autoridades policiais, os representantes de *software* ajudaram a criar novos tipos de procura institucional.”⁵² (Brayne 2017, 996).

Através do programa, *NOLA For Life*, na base de uma reunião de intervenientes com uma ação sem fins lucrativos e com o intuito de ver a taxa de homicídios reduzida com a aposta em estratégias orientadas por dados é aprovada pelo presidente Mitch Landrieu uma parceria entre o Departamento da Polícia de Nova Orleães e a empresa de software, *Palantir Technologies*. No entanto, esta parceria iniciada em 2012 escapou à supervisão dos cidadãos de Nova Orleães e ao processo de contratação pública (Winston 2018).

Pelo facto de surgir num suporte sem fins lucrativos, isto é, uma parceria com carácter filantrópico, devido ao papel que *Palantir Technologies* desempenhou, “*pro bono*”, ou seja, uma ação caritativa na oferta dos produtos da empresa para o combate à criminalidade na cidade permitiu que esta parceria saísse ilesa ao escrutínio do público, pois nunca foi devidamente comunicada à cidade, nem aos próprios membros do Conselho (Winston 2018). O acordo fechado entre as partes apenas era do conhecimento de *Palantir Technologies*, do procurador, do departamento da polícia e do presidente Mitch Landrieu, isto porque, para além das questões já referidas, este tipo de políticas ligadas às autoridades policiais locais apenas requeriam a aprovação pela figura do presidente devido ao modelo de governo característico a Nova Orleães, “*strong mayor*” (Winston 2018).

O procedimento discreto desta parceria deve-se às questões que estas novas soluções “inteligentes” geram na sociedade civil. Por não haver uma garantia à população de como são tratados os seus dados, por não haver transparência por parte das agências sobre este tipo de parcerias e, essencialmente, por não haver garantias que este novo modelo de *policing* seja realmente eficiente. O receio está, por um lado, na prolongação e aprofundamento de questões ligadas à discriminação e a práticas inconstitucionais verificadas até então e, por outro lado, no desbravar irreversível de mais um elemento que se agrega à triagem da população e se agrega ao

⁵² Tradução livre de: (...) software representatives demonstrated the use of their platform in a non-law enforcement - usually military - context, and then asked local law enforcement whether they would be interested in a similar application in their local context. In other words, instead of filling analytic gaps or technical voids identified by law enforcement, software representatives helped create new kinds of institutional demand.

conhecimento inusitado do quotidiano da mesma, a um nível que nem a própria toma consciência, o pináculo da vigilância.

Com esta parceria, o caso não foi diferente. Não foi possível um escrutínio público da parceria por evadir-se do próprio escrutínio do Conselho, por não ter sido devidamente noticiada e comunicada nos canais que chegam até à população e, pelo estatuto “*pro bono*” concedido à parceria. Isto é, devido à discrição da parceria e do seu estatuto caritativo, os membros do Conselho e o público desconheciam a sua existência pois nem estava visível nas verbas orçamentais da cidade, nem estava ao abrigo da sua fiscalização (Winston 2018).

Mas então de que forma se procedeu esta ajuda de *Palantir Technologies* ao Departamento da Polícia de Nova Orleães? Numa narrativa projetada pela empresa no combate à violência como comportamento padrão da cidade, em ajuda ao departamento, percebemos pela bibliografia disponível que tal como sucedeu com o departamento de Los Angeles, aqui também se optou pela medição do risco. No entanto, nas declarações da empresa apenas é dado um carácter interpretativo ao trabalho da mesma: “Ao trabalhar com os funcionários da cidade, estamos a ajudar a quebrar o ciclo de violência e a conduzir estratégias interventivas em várias jurisdições de aplicação da lei e programas do setor público.”⁵³; “Com *Palantir Technologies*, a cidade está a desenvolver uma melhor compreensão da sua propensão para crimes violentos e a conceber intervenções específicas para proteger as populações mais vulneráveis da cidade.”⁵⁴ (Palantir Technologies 2015). Por outro lado, temos a narrativa do gabinete do presidente da cidade Mitch Landrieu em conformidade:

“Lançada em maio de 2012, *NOLA FOR LIFE* é a estratégia abrangente de redução dos homicídios do Presidente da Câmara de *New Orleans*, Mitch Landrieu, para combater a taxa de homicídios historicamente elevada da cidade. Reconhecendo que a autoridade policial local por si só não consegue resolver o problema dos homicídios, *NOLA For Life* adota uma abordagem holística para chegar à raiz do problema e, implementa iniciativas em cinco categorias principais: parar os tiroteios, investir na prevenção, promover empregos e oportunidades, fortalecer o departamento da polícia de Nova

⁵³ Tradução livre: Working with city officials, we're helping to break the cycle of violence and drive interventions across multiple law enforcement jurisdictions and public sector programs.

⁵⁴ Tradução livre de: With Palantir, the city is developing a better understanding of violent crime propensity and designing targeted interventions to protect the city's most vulnerable populations.

Orleães (DPNO) e envolver-se, para além de reconstruir bairros.” (City of New Orleans 2013)⁵⁵

Tal como vimos com o departamento de Los Angeles existe uma aposta, também pelo departamento de Nova Orleães, nas técnicas da *actuarial justice*, isto é, uma avaliação dos riscos, por um lado dos mais propensos a cometerem algum crime e, por outro, daqueles que podem ser as vítimas. Na identificação e combate aos riscos determinantes da violência na cidade, este programa compromete-se com a redução das taxas de criminalidade, mas também, com a abordagem holística com que se imiscui, na proteção das comunidades mais fragilizadas com o suporte às infraestruturas críticas da cidade (The City of New Orleans Health Department 2013).

Como o autor Andrew Ferguson (2017, 35) sugere, há uma dualidade na ação destas autoridades públicas quando aplicam estas capacidades analíticas do software, num primeiro momento temos uma abordagem ulterior da saúde e segurança públicas em relação à violência e, na mesma medida, é adotada uma abordagem analítica das redes de interações sociais para a gestão de riscos. Com o acesso a uma miscelânea de informações, o fenómeno de *BigData* é entendido como resposta no combate à violência ao endossar uma aparente análise preditiva assegurada pelos produtos de empresas como *Palantir Technologies*.

Nesta dualidade, o departamento e a empresa conseguem definir quem são os visados e fazer uma previsão dos atingidos através da integração e visualização dos dados sobre a população de forma contextualizada. É possível compreender quase de forma exata o papel que *Palantir Technologies* teve na comunidade de Nova Orleães por uma apresentação interna, pois é identificado nesta que ao usar os dados obtidos o foco volta-se para cinco vizinhanças em particular, e em jovens, afro-americanos, essencialmente do género masculino, com baixa escolaridade e subempregados, enquanto infratores e enquanto vítimas (Schirmer, e Asher 2014, slide 6).

O departamento usufrui dos produtos da empresa para prosseguir com investigações criminais, estatuir acusações e estabelecer estratégias que permitam a redução dos homicídios por meio de uma tática definida por *Palantir Technologies*, uma *social network analysis* (ver **Anexo IV**):

⁵⁵ Tradução livre de: Launched in May 2012, NOLA FOR LIFE is New Orleans Mayor Mitch Landrieu's comprehensive murder reduction strategy to tackle the city's historically high murder rate. Recognizing that law enforcement alone cannot solve the murder problem, NOLA FOR LIFE takes a holistic approach to get to the root of the problem, and implements initiatives in five main categories: Stop the Shooting, Invest in Prevention, Promote Jobs and Opportunity, Strengthen the NOPD and Get Involved and Rebuild Neighborhoods.

“Todos os dias, análises das redes de interações sociais de vítimas e de suspeitos de tiroteios e homicídios são entregues à direção do DPNO, aos seus detetives e aos parceiros ao nível federal que estejam interessados; Gráficos *ad hoc* destas análises são fornecidos aos detetives para apoiar e ajudar a resolver investigações específicas.” (Schirmer, e Asher 2014, slide 15)⁵⁶.

Pela primeira vez registada, a empresa afirma as suas capacidades preditivas na identificação do risco na apresentação interna do seu trabalho com o DPNO ao explicar a sua aplicação de uma *social network analysis*. Estas análises começaram por integrar os dados da cidade e da sua população fornecidos pelo departamento nos anos compreendidos 2011-2013, isto é, ainda anterior à incorporação de *Palantir Technologies* (2012), sobre as vítimas mortais e não mortais de tiroteios para quantificar o risco da comunidade mais vulnerável. *Palantir Technologies* admite identificar uma taxa entre os 35% e 50% destas vítimas numa população de 3,800 cidadãos, o que corresponde a uma avaliação do risco de cerca de 1% da população total da cidade, este método foi intitulado *The NOLA Model*. Em acréscimo, com importância para o estudo de caso, temos a empresa a assumir nesta apresentação interna que é através da identificação preemptiva destas vítimas que ajudam o departamento a reduzir a população-alvo, resultando na maximização da eficiência na alocação de recursos (Schirmer, e Asher 2014, slide 18). O poder preditivo com o qual operam permite fazer uma seleção de entre a população da cidade designada de alto risco, com base em dados recolhidos pelo mesmo departamento indiciado de uma conduta inconstitucional e de práticas discriminatórias.

Ademais, a apresentação interna explicita a organização de um esforço conjunto entre os principais intervenientes, o gabinete do Presidente Mitch Landrieu e a equipa que suporta o programa *NOLA For Life* juntamente com *Palantir Technologies*, com vista a que o *NOLA Model* detenha as informações suficientes para prosseguir com as abordagens de prevenção, intervenção e reabilitação programadas pela empresa. Assim, a companhia reconhece ser capaz de reduzir a lista dos visados, semelhante à estratégia adotada pelo departamento de Los Angeles, a partir de uma conjuntura que engloba três passos essenciais: a seleção dos indivíduos que detêm os maiores indicadores de violência (idade, antecedentes criminais e afiliações a gangues); a identificação de indivíduos que já estivessem envolvidos noutros estágios do programa *NOLA For*

⁵⁶Tradução livre de: Each day, social network analyses of victims and suspects in recent shootings and homicides are delivered to NOPD leadership, NOPD detectives, and interested Federal partners; Ad hoc social network analysis charts provided to interested detectives to support and help solve specific investigations.

Life e, finalmente, com o reconhecimento de indicadores que poderiam sugerir qual a intervenção mais adequada, se por um lado a intervenção das autoridades locais ou se por outro, seriam os serviços sociais os mais apropriados ou até mesmo, a sua combinação (Schrimmer, e Asher 2014, slide 22).

Esta foi na sua base a aplicação de produtos preditivos ao Departamento da Polícia de Nova Orleães por meio de um programa suportado por uma fundação sem fins lucrativos, com recurso a *Palantir Technologies*. Esta parceria perdurou no tempo e foi estendida por três vezes consecutivas, de 2012 a 2018, evadindo-se sempre do escrutínio público até ao ano de rutura em 2018⁵⁷. O fator determinante do insucesso desta parceria, com o seu término em 2018 por retaliação do público após a revelação da parceria por parte de Ali Winston (2018), no *The Verge*, está diretamente ligado à importância da parceria, a qual se traduz na aplicação de análises preditivas e avaliação do risco de pessoas na cidade de Nova Orleães, na perpetração de crimes, com recurso a bases de dados que, para além de estarem longe da observação dos visados, podiam corresponder a dados enviesados tendo em conta as práticas institucionais: detenções ilegais, policiamento institucional, uso excessivo da força em comunidades vulneráveis (Winston 2018). Assim sendo, o corpo dos dados usados por *Palantir Technologies* levava em conta dados enviesados do departamento devido à integração de informação do próprio departamento relativa aos anos anteriores à incorporação de *Palantir Technologies*.

Há uma correlação feita pelo público e pela literatura entre o uso de dados enviesados e a população visada pelo programa com a aplicação de uma análise preditiva. A comunidade atingida pelas práticas institucionais do departamento anterior à integração de *Palantir Technologies* é, em termos práticos, a mesma comunidade sugerida pelas análises da empresa como a de maior risco na perpetração de crimes (Schrimmer, e Asher 2014, slide 6). Esta correlação traz à discussão um fenómeno ligado à integração de capacidades preditivas em agências governamentais, como as autoridades policiais locais, como é o caso do fenómeno de *dirty data*, que irá ser discutida de seguida.

Começando por identificar as fontes de dados usadas por *Palantir Technologies* para a aplicação da sua *social network analysis* verifica-se, considerando documentos apresentados pela empresa, a integração de fontes de dados primárias como sistemas de registos padrão às

⁵⁷ Documentos oficiais que mostram a assinatura do prolongamento da parceria entre o departamento da polícia de Nova Orleães e a empresa privada de software, *Palantir Technologies*, por ordem cronológica: <https://www.documentcloud.org/documents/4344819-K14-182-Palantir-Technologies-Amendment-1.html>; <https://www.documentcloud.org/documents/4344818-K16-430-Palantir-Technologies-Amendment-2.html> ; <https://www.documentcloud.org/documents/4344817-K17-453-Palantir-Technologies-Inc-Amd-3.html> .

autoridades do departamento, do *Orleans Parish Sheriff's Office* e de outras agências parceiras como chamadas de serviço, registos eletrónicos da polícia; os *Fls*; o *Case Management System*; o *National Integrated Ballistic Information Network Ballistics System*; registos de liberdade condicional de Orleães e de comunidades vizinhas; registos de detenções e reservas, para além de uma base de dados de grupos e gangues (Schirmer, e Asher 2014, slide 5). Além destas, foram também integrados vários conjuntos de dados de open source com o objetivo de proporcionar uma visão da comunidade e das infraestruturas críticas de Nova Orleães para ajudar na visualização e contextualização dos dados, tais como: detalhes de localização e características descritivas de escolas, hospitais, bibliotecas, iluminação pública e outras infraestruturas cívicas; registos de lojas de bebidas alcoólicas; registos de câmaras privadas residenciais e comerciais e, mapas essenciais da cidade (Palantir Technologies 2014).

A somar a isto, a empresa divulga ainda nesta apresentação interna, o uso e integração de dados de chamadas feitas na prisão e dados dos telemóveis, para além de dados obtidos pela análise das redes sociais e publicações nas mesmas da população visada (Schirmer, e Asher 2014, slide 14). De modo a sumarizar a questão que se coloca, o modelo preditivo de *Palantir Technologies* na cidade de Nova Orleães utilizou uma técnica de *intelligence*, uma *social network analysis*, para estabelecer ligações entre pessoas, locais, armas, moradas e até, publicações nas redes sociais e outros indícios em bases de dados anteriormente isoladas e inacessíveis⁵⁸. Tal como na instância anterior, a plataforma funciona através da introdução de um termo de consulta, um *query term*, como por exemplo, uma matrícula parcial, uma alcunha, uma morada, um número de telemóvel, uma identificação ou publicação nas redes sociais, que iria proporcionar ao analista do departamento uma agregação de dados que lhe permitia determinar quais os indivíduos de maior risco na prática de violência ou de se tornarem nas vítimas, com base na sua ligação a vítimas ou agressores já conhecidos do departamento (Winston 2018). O reconhecimento do uso e análise de redes sociais da população, se assim for conhecido, ligado à avaliação do risco da própria para uma ação mais eficiente por parte de *law enforcement* pode trazer consequências para o exercício dos direitos dos cidadãos, ao reprimir o discurso, a organização e a discordância (Stanley 2018). Percebemos que, através de uma permuta de informação entre os atores, por um lado o acesso à plataforma e dados de *Palantir Technologies*, por outro lado a concessão do acesso

⁵⁸ Quando do estabelecimento da parceria em 2012, o presidente Mitch Landrieu assinou um acordo onde concede formalmente às autoridades da cidade de Nova Orleães o acesso gratuito à plataforma de integração de dados do setor público da empresa: <https://www.documentcloud.org/documents/4344821-K12-168-Palantir-Technologies.html> (Winston 2018).

e análise a bases de dados criminais e não-criminais do departamento, permitia a instrução do software ao capacitar a sua previsão de crimes (Winston 2018).

Voltando à questão que se coloca com esta parceria, após uma análise dos dados utilizados na fusão de sinergias entre o departamento de Nova Orleães e *Palantir Technologies*, irá ser analisado de seguida o fenómeno de *dirty data*, em evidência.

Os dados utilizados pelo departamento no período da parceria com o departamento são dados que refletem práticas e viés do próprio departamento antes da integração destas tecnologias, como referido anteriormente. Apesar de não haver uma correlação direta entre os dados utilizados e o viés que se verifica na comunidade mais atingida por este *predictive policing*, também não há na prática, uma garantia de que as partes se certificaram de que os dados do departamento integrados no sistema de *Palantir Technologies* fossem “limpos” de erros e irregularidades ou alterados à luz dos dados “sujos” identificados no relatório do departamento de Justiça. Esta questão demonstra o risco elevado associado ao produto de *Palantir Technologies* usado para decifrar e triar a população de Nova Orleães no uso de *dirty data*, pois já verificado anteriormente, na análise do sistema usada na apresentação interna acima explorada, encontram-se disparidades raciais semelhantes. Mas, devido à falta de transparência e da possibilidade de uma supervisão por parte da população e da ausência de uma autoridade legislativa que fiscalize esta atividade, não há certezas quanto ao grau de viés existente e o risco a ele associado na população de Nova Orleães (Richardson et al. 2019).

Tal como na parceria com o Departamento da Polícia de Los Angeles, aqui, com o departamento da polícia de Nova Orleães verifica-se uma falta geral de transparência pública relativamente ao policiamento e aos sistemas de policiamento preditivo, o que dificulta o traçar de uma linha reta entre a *dirty data* produzida pelo departamento na jurisdição de Nova Orleães e os sistemas designados *predictive* utilizados. Por estes motivos, é sugerido pela bibliografia que as práticas inconstitucionais e litígios que daí resultaram por parte deste departamento fizeram parte do policiamento preditivo alcançado por meio da empresa privada. O que se sabe é que na prática, não existem procedimentos regularizados e métodos normalizados na recolha, avaliação e utilização de informações recolhidas no curso da ação das autoridades da polícia e, que, as práticas policiais estão fundamentalmente desligadas dos controlos democráticos⁵⁹ (Richardson et al. 2019).

⁵⁹ Pela fragmentação que existe no mosaico de leis federais quanto à privacidade nos EUA que traz dificuldades para a regulamentação da atividade de empresas privadas, mas também na atividade de agências governamentais. Dentro destas leis existem algumas que restringem a recolha direta

Ao analisar o uso destas parcerias para combater taxas de criminalidade verifica-se que estas capacidades preditivas, a que o público não tem acesso, estão inseridas no processo de tomada de decisão, e no caso de serem parcerias no âmbito do policiamento da população e justiça penal, incluindo processos de acusação, pré-julgamento, sentença, liberdade condicional e correções, leva a um questionamento importante que deve ser alvo de investigações como esta. Se os processos de tomada de decisão de *law enforcement* passam por produtos preditivos e algorítmicos, que são *black-boxed* (ver **Anexo V**), que derivam as suas análises da população de dados policiais, que são muitas vezes enviesados, tal como vimos, torna-se necessário e uma condição sine qua non um exame e uma reforma mandatária das práticas de policiamento e, uma análise dos dados que funcionam como registo dessas práticas para uma discussão informada sobre os possíveis danos e benefícios dos sistemas de policiamento preditivo de terceiros cujas conclusões são moldadas por esses dados (Richardson et al. 2019).

É de notar que a parceria com *Palantir Technologies*, no seio da grande estratégia de redução de crime da cidade *NOLA For Life*, incluía ainda esforços de dissuasão de criminalidade, tal como na parceria anterior, com base num projeto intitulado *CeaseFire Program*, que estava inserido dentro da estratégia matriz. Este programa era uma estratégia “carrot and stick” em que as forças da ordem policial informam os prováveis infratores, de acordo com a informação proporcionada por *Palantir Technologies*, de que têm conhecimento das suas ações e registos passados e que, como consequência, vão processá-los ao máximo se existir reincidência. Se este grupo de pessoas estiver disposto a cooperar, são chamados para uma reunião obrigatória como parte das suas condições de liberdade condicional e, é-lhes oferecida formação profissional, educação, possibilidade de colocação profissional e ainda, serviços de saúde (Winston 2018). Como referido acima, a abordagem da parceria era holística, com vista a atender vários pontos problemáticos da cidade, o que incluía este programa de combate à reincidência, mas não só. Com base na análise de *Palantir Technologies*, os bombeiros aumentaram a sua presença em algumas escolas particulares, o departamento da saúde debruçou-se sobre escolas de alto risco para a prevenção da violência e a polícia fez o mapeamento das áreas mais problemáticas. A autoridade responsável pela fiscalização do consumo de bebidas alcoólicas centrou-se nas

de informação pessoal identificável por parte do governo como por exemplo, *The Privacy Act* (1974); *Electronic Communications Privacy Act* (1986); *Telephone Records and Privacy Protection Act* (2006) e *Video Protection Privacy Act*, entre outras. No entanto, estas leis não impedem o acesso das autoridades policiais, tal como nos diz Erin Murphy (2013) citado por Ferguson (2017, 17): “*The U.S. code currently contains over 20 separate statutes that restrict both the acquisition and release of covered information (...) Yet across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms.*”. A polícia pode obter certos dados através de uma ordem judicial ou intimação, com um mandado válido, a polícia pode obter quase tudo o que as grandes empresas de dados tenham recolhido para fins de consumo.

violações que ocorrem nas lojas e, ainda, a limpeza de ruas em certas vizinhanças. Os mesmos dados que tinham em vista mapear o crime, serviram para dirigir serviços governamentais e infraestruturas públicas (Ferguson 2017, 41). Aqui, é possível denotar o *social sorting* de que fala David Lyon, pelo meio da vigilância, as agências governamentais conseguem atingir o seu fim: gerir os indivíduos de risco, atribuindo-lhes um valor, ao mesmo tempo que criam e reforçam as diferenças sociais que anseiam, a longo prazo (Lyon 2003).

De acordo com a análise de algumas fontes, é possível perceber alguns resultados desta estratégia de redução de crime aplicada pela cidade de Nova Orleães, no entanto, o impacto efetivo da parceria e da ajuda e análise de *Palantir Technologies* no combate à taxa de criminalidade não é possível determinar, devido à sua falta de transparência na forma em que procede e por estar ausente da consciência da população.

Na avaliação formal desta parceria, por parte do Departamento de Justiça dos EUA, é feito um estudo do impacto a longo prazo da estratégia de *focused-deterrence* na cidade de Nova Orleães, com foco na documentação das mudanças ao nível de homicídios e recuperações de armas de fogo, estratégia que se mostrou beneficiar dos produtos de *Palantir Technologies*, no entanto, não é feita menção à mesma. Nesta avaliação, os autores concluem o estudo dizendo que a estratégia de redução da violência aplicada a Nova Orleães esteve ligada de forma significativa à redução da violência com armas de fogo na cidade no entanto, é feita uma ressalva de que se evidenciou na continuação da intervenção uma erosão dos benefícios ou uma diminuição dos retornos da intervenção, isto é, o uso da estratégia *focused-deterrence* apresenta problemas quanto à sua durabilidade na medida em que, não se vê uma sustentabilidade da estratégia a longo prazo (Corsaro et al. 2018).

Depreende-se que não é possível fazer uma avaliação do impacto real das parcerias entre as agências governamentais e as empresas na ótica do policiamento preditivo uma vez que, para além de serem parcerias asseguradas pelo sigilo, a forma como funcionam estas capacidades das empresas de software também ainda não foram desmistificadas. No entanto, estes produtos estão a ser implementados e usados há algum tempo ainda que não haja uma avaliação real das suas implicações para a população, não só ao nível da falta de transparência no uso dos dados, mas também ao nível da segurança pública visto que, o uso de dados enviesados pode refletir a contínua discriminação de um nicho da população. E, apesar de ser atribuído a estes produtos um nível de eficácia exímio por não derivarem inteiramente da racionalidade humana, não é possível comprovar diretamente esse impacto positivo.

Quando a parceria do departamento de Nova Orleães com *Palantir Technologies* foi trazida a público por Ali Winston através da plataforma *The Verge*, em 2018, seguiu-se uma reação pública negativa devido à natureza secreta dessa mesma parceria e pela insciência sobre os termos em que atuava. No mês seguinte à revelação, a parceria com *Palantir Technologies* é terminada quando o gabinete de imprensa do presidente Mitch Landrieu comunicou ao jornal da cidade, na altura, o *The Times-Picayune*, que não iria renovar o contrato “pro bono” com *Palantir Technologies*. Foram as primeiras observações do gabinete do presidente da cidade em relação ao trabalho conjunto do departamento com *Palantir Technologies* (Bullington, e Lane 2018).

De forma a concluir a análise desta parceria é importante refletir, novamente, sobre o grande problema que se apresenta com o uso de parcerias entre agências governamentais e empresas de software para calcular o risco da população em termos de violência, problema que acresce aos apresentados na parceria anterior, na parceria entre o departamento de Los Angeles e *Palantir Technologies*. Assim, na análise desta parceria em particular verifica-se uma assunção comum a outras em que o uso de dados policiais e bases de dados criminais são usados como indicadores de padrões reais de comportamento da população. No entanto, é possível inferir que neste caso, há um viés associado aos registos da polícia devido à confirmação de discriminação e práticas institucionais por parte do departamento. Com isto, assumir os dados das autoridades policiais locais como objetivos é uma distopia que se apresenta para aqueles que terão de experienciar a aplicação de *dirty data* nas suas vidas.

Os dados refletem práticas, políticas, preconceitos e necessidades político-financeiras de um determinado departamento. Neste caso em particular, a probabilidade de se verificar preconceitos raciais, a falta de transparência, os erros dos dados apresentam-se como fatores que vão defraudar os resultados das estratégias de avaliação do risco da população e como fatores que questionam a verdadeira eficácia e imparcialidade dos produtos orientados por dados, que prometem antecipar-se ao risco de existir outro crime na cidade. A bibliografia mostra que quando existe *dirty data* no sistema esta é frequentemente sistémica e generalizada, pelo que qualquer que seja o método que pretende evitar ou atenuar o impacto desta em sistemas preditivos tecnológicos, vai ter dificuldades em demonstrar que estes dados enviesados foram completamente dissecados e eliminados da análise preditiva, no entanto, estão, ainda assim, a servir atualmente como estratégias para assegurar a segurança pública por estes organismos governamentais. Isto levanta o questionamento sobre os termos em que o direito fundamental à segurança pública está a ser garantido e, por isso, torna-se, importante, conhecer realmente e

tornar transparente a análise e os dados utilizados por estas parcerias na apreciação do risco da população.

A corrente atual que se verifica no âmbito do *policing* é de um governo por algoritmo que encaixa no fenómeno da “algocracia” situação em que os sistemas baseados em algoritmos estruturam e limitam as oportunidades para a participação da população na tomada de decisões públicas, tal como na compreensão das mesmas o que representa uma ameaça premente que deve ser resistida (Danaher 2016, 246). Contudo, não deixa de ser notável a importância destes produtos assegurados por empresas como *Palantir Technologies*, tal como é sugerido por Andrew Ferguson (2017, 58), que deixa algumas notas positivas sobre um cenário promissor quanto à utilização de *BigData* para o futuro de *law enforcement*, ao indicar que se por uma ínfima fração a análise destes grandes volumes de dados conseguir separar as pessoas de maior risco das de menor risco, ganha-se algum grau de eficiência. Para além disso, mesmo existindo interesses próprios e agendas a cumprir pelas partes, a capacidade de priorizar de forma “inteligente” quem deve ser investigado é uma ferramenta tecnológica muito apelativa, sem esquecer os requisitos de transparência e responsabilização que devem ser assegurados.

No decurso destas parcerias, Palantir Technologies conseguiu patentear um sistema de previsão de crime, tornando pública a sua capacidade efetiva quanto ao método de *predictive policing*.

“Visão geral: Os departamentos da polícia e outras agências de aplicação da lei gostariam de saber quando e onde os crimes são mais prováveis de ocorrer no futuro, a fim de afetar de forma mais eficiente e eficaz os recursos de prevenção de crime. Um sistema ‘*computer-based*’ de previsão de risco de crime e o método correspondente são fornecidos para gerar previsões de risco de crime e transmitir essas mesmas previsões a um utilizador. O utilizador pode ser por exemplo, um agente da polícia ou outro funcionário responsável pela aplicação da lei. Com as previsões transmitidas, o utilizador pode avaliar mais eficazmente o aumento do nível da ameaça de crime e a sua potencial duração. O utilizador pode, então, aproveitar as informações transmitidas pelas previsões para adotar

uma abordagem mais pró-ativa a *law enforcement* nas áreas afetadas durante esse período de ameaça de crime.” (Robertson, et al. 2015, 2)⁶⁰.

É possível verificar uma outra situação em que o uso destes produtos das empresas de software determina a avaliação governamental sobre os imigrantes, um caso controverso com a agência *ICE*, novamente em colaboração com *Palantir Technologies*, que irá ser abordada de seguida.

3.3. A cooperação de *Palantir Technologies* com a agência: Imigração e Alfândega dos EUA (*ICE*)

3.3.1. Plataforma *Investigative Case Management (ICM)* na cooperação com *Palantir Technologies*

Esta infraestrutura vigilante de informação que se mostra vital à ação destas agências governamentais, verifica-se, ao longo da análise desta cooperação como a principal ferramenta atual para o decurso de *law enforcement*, ao incorporar vários fluxos de informação e de ligações entre vários sistemas de informação apresentando, posteriormente, a informação de forma contextualizada aos utilizadores da plataforma *ICM*. Estas competências compõem um regime de mapeamento de informação crucial ao aparelho securitário dos EUA. Isto é, permite aos agentes de várias divisões do governo, a autoridade delegada de conduzir o decurso e os resultados da imigração na forma como visualizam a informação disponibilizada e analisada nessa mesma plataforma (Knight e Gekker 2020, 232).

De modo a iniciar a análise da última parceria, deve-se mencionar que o foco nesta fase não está voltado para o fenómeno até aqui desenvolvido do *predictive policing*, mas sim, ainda dentro do espectro de *law enforcement* está voltada antes para a acumulação de informação que é alcançada pela parceria público-privada. Para além disso, neste caso em particular, remonta-se à questão securitária que descreve o mote dos EUA no que se refere à vigilância massificada de cidadãos e não-cidadãos e de como, esta mesma vigilância já não é separável de infraestruturas tecnológicas que ditam aos agentes de *law enforcement* o que se sabe sobre a vida das pessoas, agindo em condescendência com a apreciação dos produtos algorítmicos e de *machine-learning*.

⁶⁰ Tradução livre de: Overview: Police departments and other law enforcement agencies would like to know when and where crimes are most likely to occur in the future in order to most efficiently and effectively allocate crime prevention resources. A computer-based crime risk forecasting system and corresponding method are provided for generating crime risk forecasts and conveying the forecasts to a user. The user may be a police officer or other law enforcement official, for example. With the conveyed forecasts, the user can more effectively gauge both the level of increased crime threat and its potential duration. The user can then leverage the information conveyed by the forecasts to take a more proactive approach to law enforcement in the affected areas during the period of increased crime threat.

Até este ponto da investigação foram referidos casos em particular de agências locais de *law enforcement* e a sua utilização de produtos tecnológicos na avaliação do risco da população, no entanto, nesta fase da investigação, a atenção centra-se ao nível federal da abordagem de *law enforcement* com a análise da parceria entre *Palantir Technologies* e a agência governamental *ICE*.

O mote securitário está na aposta em forças de segurança no combate ao crime e à atividade terrorista em todas as frentes do país no pós-11 de setembro, a criação do próprio Departamento de Segurança Interna dos EUA partiu daí. É possível verificar o custo das tremendas reformas no aparelho de segurança dos EUA entre 2002 e 2017, num valor estimado de 2.8 trilhões de dólares gastos em iniciativas e esforços de contraterrorismo (Heeley et al. 2018 citado por Knight e Gekker 2020, 234).

O Departamento de Segurança Interna dos EUA é a maior agência ao nível federal de *law enforcement*, com cerca de 80.000 agentes que executam as missões do departamento através de nove agências e gabinetes diferentes. Dentro das missões deste departamento assinala-se a: segurança das fronteiras terrestres e marítimas dos EUA; manter possíveis terroristas e as suas armas fora do país; proteger o comércio e as viagens internacionais; aplicação das leis civis e criminais em matéria de alfândegas, comércio e imigração; salvaguardar a infraestrutura financeira da nação; investigação de crimes e ameaças transnacionais; formar os agentes federais de *law enforcement* da nação; proteger as instalações federais, os funcionários e os visitantes; e, assegurar a continuidade das operações governamentais. A ação deste departamento é conseguida através do envolvimento próximo com o público e, através de fortes parcerias entre as partes interessadas ao nível federal, estatal, local, territorial e internacional que reúnem esforços para garantir a segurança de todas as comunidades visadas (Departamento de Segurança Interna dos EUA 2023). Dentro das várias divisões que compõem os elementos operacionais e de apoio deste departamento verifica-se a agência governamental *ICE* da alçada do *DHS*, relevante para o contexto da dissertação.

ICE é outra das várias agências no enquadramento de *law enforcement*, mas que, por sua vez, se foca no tema da imigração. A sua missão pela perspetiva da própria agência passa por proteger o país levando a cabo investigações criminais e garantindo a aplicação no terreno das leis de imigração de modo a preservar a segurança nacional e pública. Tem em vista a mitigação de ameaças transnacionais e procura salvaguardar a nação, as suas comunidades, a imigração legal, o comércio, viagens e sistemas financeiros (Imigração e Alfândega dos EUA 2023).

Ainda dentro desta agência governamental existem duas abordagens distintas, mas complementares em relação à imigração. De um lado, *Enforcement and Removal Operations (ERO)*, mais direcionada para a responsabilidade sobre a deportação. Um dos esforços mais notáveis de coordenação e parceria entre estas forças no âmbito do *ERO* envolve a identificação biométrica e biográfica de indivíduos indocumentados que estão encarcerados em prisões e cadeias federais, estatais e locais. Trabalha de perto com os vários parceiros e agências responsáveis pelo *law enforcement* espalhadas pelo país no que diz respeito à responsabilidade partilhada em garantir a segurança das comunidades do país através de um conjunto de recursos e programas. Destes, destaca-se o programa 287 (g) que concede a estas entidades, sejam elas estatais ou locais, uma autoridade delegada, formação e recursos tecnológicos para a aplicação das leis de imigração nas suas jurisdições. Esta agência governamental permite o aumento do impacto das forças de intervenção dos vários gabinetes do país através da sua autoridade administrativa para prender indivíduos considerados uma ameaça à segurança pública devido ao seu estatuto de imigração ilegal, sem acusações criminais adicionais. Com o recurso a parceiros como a *INTERPOL* e *ICE Attaché corps*, a conjuntura das *ERO* desenvolve pistas de investigação e presta auxílio na localização e detenção de cidadãos estrangeiros procurados por crimes cometidos no estrangeiro que se encontram atualmente em liberdade nos EUA (Imigração e Alfândega dos EUA 2023). Por outro lado, a divisão *Homeland Security Investigations (HSI)*, que está voltada para o combate ao crime transnacional, ao focar-se em crimes transfronteiriços mais graves, como casos relacionados com terrorismo e o tráfico de seres humanos (Woodman 2016). Uma componente crítica à segurança pública, a divisão das *HSI* investiga redes criminosas que se dedicam a atividades ilícitas como o contrabando de estupefacientes, o tráfico de seres humanos, violência de gangues, o branqueamento de capitais e outros crimes financeiros, o roubo de propriedade intelectual e a fraude aduaneira. Para além disso, também investiga crimes cibernéticos, incluindo a exploração de crianças, com o objetivo de proteger as fronteiras físicas e virtuais. Esta divisão é a maior contribuinte para as *FBI-led Joint Terrorism Task Forces* e utiliza as suas autoridades particulares e exclusivas em matéria de imigração e comércio para dismantelar redes terroristas e prevenir ataques contra a pátria (Imigração e Alfândega dos EUA 2023).

Percebe-se com esta apreciação da missão da agência *ICE* que o seu peso na avaliação do risco à segurança do país é determinante na cadeia das forças de segurança dos EUA, principalmente na abordagem da imigração. Assim, de modo a montar o palco para analisar a parceria aqui em questão, refere-se o enquadramento da reforma das unidades de segurança. O

programa *TECS Modernization*, finalizado em 2011, é um esforço da agência matriz de *law enforcement*, *DHS*, para modernizar os principais sistemas de gestão de processos de aplicação da lei e reforçar a sua ação. Foi uma iniciativa com vista a substituir o antigo programa *TECS*, um sistema primário de controlo das fronteiras que apoia o rastreio dos viajantes que entram nos EUA, bem como os requisitos de rastreio de outras agências governamentais. O *case management system* permite a interação com os vários sistemas e agências de *law enforcement* espalhados pelo país e é fruto de um esforço conjunto das divisões *ICE* e *U.S. Customs and Border Protection (CBP)*, com vista a apoiar a continuação das missões de cada agência aqui referida (Departamento de Segurança Interna dos EUA 2010). De modo a melhorar a gestão do fluxo de pessoas nos portos de entrada fronteiriços e a gestão dos casos de aplicação das leis de imigração, o *DHS* investiu na modernização deste programa informático que serve agora o propósito de ambas as agências acima mencionadas.

Este programa apoia a gestão de casos de investigação da divisão *ICE*, inclusive a documentação de objetos de investigação criminal na forma de registos e relatórios para a formação de uma base robusta para os processos penais (Imigração e Alfândega dos EUA 2014). No entanto, estes esforços não estavam refletidos em resultados e foi necessária uma nova avaliação que resultou na contratação por parte desta agência governamental, *ICE*, de *Palantir Technologies* para o desenvolvimento de uma nova plataforma que acompanhasse os objetivos do programa inicial *TECS Modernization* (Imigração e Alfândega dos EUA 2014). Ao assinar um contrato estimado no valor de 53.1 milhões de dólares com *Palantir Technologies* (ver **Anexo VI**), em 2014, *ICE* estava a adotar uma solução híbrida conhecida por *COTS/Custom*⁶¹ para que a empresa desenvolvesse uma plataforma eficiente e atualizada disponível para as autoridades, um software intitulado por *Investigative Case Management (ICM)* (Mijente 2018; Knight e Gekker 2020, 235).

Esta plataforma desenvolvida por *Palantir Technologies* representa um ponto-chave no desenvolvimento da ação da organização governamental que é o *ICE*, na medida em que vai permitir uma agregação de componentes à *intelligence* do governo. Esta solução apresentada pela empresa representa, agora, a principal ferramenta para o *law enforcement case management* usado pela divisão das *HSI* pois, como antes referido, o departamento renovou o contrato com *Palantir Technologies* em 2022 por um período de 5 anos (Mijente 2018; Palantir Technologies 2022).

⁶¹ Quando os produtos já no mercado são adaptados às necessidades da organização compradora.

De notar que, para além desta ferramenta que vamos analisar em maior detalhe de seguida, esta divisão do departamento de segurança interna dos EUA usufruiu de outras ferramentas construídas pela empresa como a plataforma Gotham, a base de dados e plataforma analítica *FALCON Search and Analysis System*, que auxilia os agentes na análise de todos os dados ingeridos, a identificar ligações e a produzir relatórios e visuais de informação e, ainda, um outro software de análise conhecido por *Analytical Framework for Intelligence (AFI)*, controverso por estar ligado a algoritmos de definição de perfis (Knight and Gekker 2020, 235).

Numa fase inicial da implementação da plataforma *ICM* é anunciado num documento oficial da agência governamental *ICE* o conjunto de objetivos que se propõe a atingir por meio deste software: a criação e gestão de casos e documentos de investigação das divisões *ICE/HSI*; a criação e gestão dos registos sobre assuntos dedicados a informações relacionadas com pessoas, embarcações, veículos, aeronaves, empresas e outras; interligar os registos com os relatórios de investigação, ou os *ROIs (reports of investigation)* e com os casos em investigação; criação e gestão de registos de vigia partilhados com a divisão *CBP*; realização de pesquisa voltada para a investigação através do sistema de interfaces internos e externos à divisão *ICE* e ao *DHS*; gestão das estatísticas de casos avaliados pela agência, como detenções e apreensões; a recolha de dados administrativos como o número de horas de trabalho dos agentes nos casos e, finalmente, gerar relatórios que transmitem os dados relacionados com os casos (Imigração e Alfândega dos EUA 2014). Ainda que o uso deste software da empresa tenha sido anunciado neste documento que seria primordialmente direcionado para agentes que compõem as *HSI*, isto é, centrados no combate à atividade terrorista e, não havendo menção à divisão voltada para a deportação, *ERO*, analisa-se mais à frente, na exploração da cooperação, que contrariamente ao documento inicial, para além da plataforma *ICM* integrar a base de dados que pertence à agência *ERO*, esta última vai fazer uso dessa mesma plataforma para levar a cabo a sua missão (Woodman 2017).

Este sistema de gestão de casos, *ICM*, funciona como um repositório de informações de várias bases de dados e de várias agências do governo para além de incluir informação proveniente da área comercial e setor privado (Mijente 2018). Sendo assim, *ICM* descreve-se como a aplicação de uma plataforma personalizada que permite a criação e gestão dos processos de investigação e que veio proporcionar funcionalidades melhoradas ao módulo *TECS*, as quais incluem: uma interface atualizada que facilita as interações dos seus utilizadores; capacidades de pesquisa avançada que permitem consultas estruturadas e não estruturadas sobre os objetos de interesse;

simplificação de dados para um registo sólido; capacidades de fluxo de trabalho para apoiar a revisão e aprovação internas de casos e, a colaboração melhorada dentro da estrutura da divisão governamental, *ICE* (Departamento de Segurança Interna dos EUA 2016).

Esta plataforma de agregação atípica de informação e de uma completude inigualável da mesma, utilizada pelo próprio governo do país, integra informações de identificação pessoal bem como sobre a rede de contactos dos visados, particularidade a que assiste nas parcerias anteriores, como informações sobre os alvos de investigações, associados a estes, vítimas, testemunhas, informadores e de terceiros (Departamento de Segurança Interna dos EUA 2016).

De acordo com o documento oficial disponibilizado pelo *DHS*, “*Privacy Impact Assessment for ICE Investigative Case Management*”, de 2016, é possível depreender quais as informações que são integradas e visualizadas pelos utilizadores desta plataforma, evocando novamente a titularidade da plataforma a *Palantir Technologies*, uma empresa de software. Desde dados biográficos, que incluem mas não se limitam ao nome, data de nascimento, número de segurança social, número de identificação de estrangeiro, ou *Alien Registration Number*, número de telemóvel, dados relativos à carta de condução, ao passaporte, registo criminal bem como o estatuto e historial de imigração; contém dados descritivos, como a cor de olhos, cor do cabelo, altura, peso e outras características físicas únicas como é o caso de tatuagens, marcas e cicatrizes; dados financeiros, incluindo dados sobre atividades financeiras suspeitas, transações de divisas e relatórios sobre os instrumentos monetários; provas e respetivas descrições obtidas durante as investigações, incluindo declarações dos almejados, de testemunhas, assim como também inclui fotografias, e-mails, registos telefónicos, registos bancários, histórico de viagens, entre outros documentos relacionados; e, ainda dados relativos à localização, que provêm da observação próxima de agentes e oficiais durante atividades de vigilância ou de relatos de testemunhas e, pela utilização de instrumentos e tecnologias próprias da atividade vigilante, como ferramentas de localização que incluem dispositivos de rastreamento de localização que se encontram ocultos, informação que vai ser apresentada posteriormente aos agentes através de mapas em tempo real. E os *ALPRs*, tecnologia destacada também nas cooperações supramencionadas, que constituem dados conseguidos através de câmaras de vigilância operadas pelo *ICE* durante uma investigação, ou obtidos em resultado de iniciativas conjuntas com parceiros policiais, estes dados incluem imagens de matrículas de veículos associados a um alvo de investigação, data e hora, e coordenadas *GPS* do local onde a matrícula foi fotografada; finalmente, a plataforma tecnológica agrega dados de telecomunicações, como identificadores de dispositivos, dados de utilização e

informações biográficas sobre alvos de investigação e as suas redes, registos sobre as chamadas telefónicas (data e hora, duração, número marcado, entre outras), nomes, moradas e números de telemóvel e, nalguns casos, detalhes de mensagens de texto (Departamento de Segurança Interna dos EUA 2016). No documento é identificado pela agência que em todos estes casos existe a possibilidade de conter informações pessoais identificáveis, o que permite na gestão desta plataforma um maior controlo sobre o risco, para além de que se agrega à teia governamental de dados que vão para além daqueles imediatamente necessários à investigação, pela integração de várias bases de dados, internas e externas ao *ICE*.

As bases de dados integradas na aplicação da plataforma *ICM* incluem os sistemas das divisões *ICE*, *CBP*, o *National Crime Information Center (NCIC) do Federal Bureau of Investigation (FBI)*, ao comunicar, também, com outras agências de *law enforcement* ao nível federal, estatal e local. E, são ainda intersetadas fontes comerciais, direta ou indiretamente, de forma a aceder à informação pública na *Internet*, incluindo o acesso a redes sociais no decorrer de investigações podendo, assim, incorporar essas informações nos processos. No caso de operações encobertas, podem ser recolhidas informações que não estão disponíveis ao público e, que, só podem ser visualizadas por aqueles que se ligaram com a pessoa de interesse nas redes sociais, ou a quem foi concedido esse acesso, são casos particulares de operações secretas autorizadas no decurso de uma investigação criminal (Departamento de Segurança Interna dos EUA 2016; Mijente 2018).

Este cruzamento de informação equipara-se a um mapa de interfaces, conceito já mencionado anteriormente. Interfaces funcionam como elementos de contacto entre sistemas que não podem ser ligados diretamente e permite a comunicação entre entidades, são o elemento que arbitra o significado entre sistemas e bases de dados e impulsiona, ao intersectá-los, a sua interação contínua. Assim, estes interfaces funcionam como *technical information machines* que servem para simplificar sistemas complexos, como é o caso de softwares que envolvem algoritmos, permitindo aos utilizadores destas plataformas de interpretar a informação disponibilizada (Knight e Gekker 2020, 233).

Criando uma base robusta de regimes de interfaces, os utilizadores desta plataforma conseguem ter uma visão holística e totalizante da informação que existe sobre as pessoas no sistema e, à medida que as interfaces interagem pela comunicação entre bases de dados apresentam o que está disponível e o que é relevante à pesquisa dos seus utilizadores numa extremidade da cadeia governamental impactando, de forma consequencial, a forma como estes

vão interagir com o meio em que atuam pela informação que acabaram de interpretar, produzida pelo software da empresa privada (Knight e Gekker 2020, 233).

De forma quase invisível, mas de certo inconsciente, vai existindo uma rede de interseção de informação fruto do acesso a bases governamentais, comerciais e privadas sobre os vários aspetos da vida dos indivíduos que já não é possível de antecipar, mas também, impossível de reverter pelo facto de compor o regime atual de vigilância no qual o governo se apoia para assegurar a sua segurança e a segurança pública. Isto acontece devido ao mérito que as empresas privadas de *software* abarcam com o seu desenvolvimento de plataformas como a *ICM*, com as quais os governos já não se conseguem dissociar, nem mesmo superar por conta própria, tal como também foi explicado na entrevista com *Palantir Technologies*. O *lobbying* da narrativa: “*the power of the best minds of the private sector*” (Amoore 2011 citado por Knight e Gekker 2020, 234).

O argumento acima apontado está em linha com a visão de Andrew Ferguson, ao assinalar o fenómeno mecânico de expansão e interligação entre a informação existente sobre a população:

“Uma vez recolhidos os dados num local, torna-se cada vez mais difícil não agregar a informação. Os dados do setor privado passam a fazer parte dos registos públicos e, em seguida, estes registos tornam-se os blocos de construção das bases de dados privadas e governamentais. Os dados são transacionados e recompilados de tal forma que o ponto de recolha original fica camuflado.”⁶² (Ferguson 2017, 18).

O foco da análise desta última cooperação, entre *Palantir Technologies* e agência *ICE*, está nas interfaces que compõem a rede de dados da plataforma *ICM* e, por isso, na forma como este software permite aos agentes de *law enforcement* de atuar através da sua operacionalização de risco de seres humanos através da informação disponibilizada pela plataforma que permite a visualização do que é conhecido como *data doubles* e *dividuals*. No artigo de Emma Knight e Alex Gekker é citada a noção de Gilles Deleuze (1992) de *dividuals* em que, o poder hodierno descreve-se como aquele que governa os comportamentos dos *dividuals* cujas identidades e ações são infinitamente divisíveis e reduzidas a coleções de dados pela tecnologia moderna. Assim sendo, à medida que a tecnologia se torna onnipresente e essencial, questão trazida ao longo da

⁶²Tradução livre de: Once data has been collected in one place, it becomes harder and harder not to aggregate the information. Private data becomes part of public records, and then public records become the building blocks of private and government databases. Data gets sold and repackaged such that the original collection point becomes obscured.

dissertação , o mesmo acontece com a “segmentação e racionalização de gestos minúsculos da vida quotidiana”, o que vai, consequentemente, facilitar as representações digitais da vida da população através de séries de dados codificados e interrelacionados, em que os utilizadores destas plataformas tecnológicas entendem ser a representação tangível da complexidade humana, estas representações são chamadas de *data doubles* (Knight, e Gekker 2020). O cume do poder reside atualmente em redes, computadores, algoritmos, informação e dados. Posto isto, as interfaces e regimes de interfaces que aqui se apresentam constituem a tradução do que é um elemento crucial na evidência de poder - acesso à informação - em que existe paralelamente uma divisão de aprendizagem dessa mesma informação, informação a que o governo e as empresas privadas têm acesso versus a informação a que a população tem acesso (Zuboff 2019).

De forma a trazer, visualmente, a simplificação das interfaces e sistemas que operam por meio da plataforma *ICM*, é possível verificar nos **Anexos VII e VII**, de forma condensada, a interoperabilidade dos principais sistemas de “*case management*” e das autoridades responsáveis pela aplicação da lei.

Considerando o relatório do grupo Mijente (2018) e a apresentação oficial: *ICE TECS Modernization Industry Day* pela agência governamental *ICE* (2023, slide 18), é possível depreender que estas interfaces e sistemas de informação que compõem a plataforma de agregação de informação, *ICM*, são transmitidas para a Amazon, mais concretamente, para o seu *software* ao serviço destas entidades: Amazon *Web Services*, devido às vantagens que os serviços de computação em nuvem proporcionam, como o armazenamento colossal de dados, sem que haja a necessidade de supervisão ativa direta de um utilizador. É mais um evento da transição em massa de informação sobre a população para uma terceira entidade, um evento mais preocupante ainda por corresponder a informação detalhada trazida por estas agências governamentais para uma entidade privada comercial, como a Amazon *Cloud Computer Services*.

A Amazon *Web Services* e *Palantir Technologies* são também uma parceria já definida, identificada no site oficial da última e, por esse motivo, a inclusão da Amazon nesta parceria mais alargada não traz estranheza. No entanto, como se verificou pela entrevista com um responsável da equipa de *Palantir Technologies* as políticas de privacidade podem não ser 100% compatíveis e, por isso, torna-se uma parceria na base de uma abordagem capacidades – expectativas. A somar a esta última questão, é possível identificar ainda, alguns casos recentes de demonstrações de violações de privacidade por parte da *Amazon*, o que traz uma preocupação acrescida ao caso, como por exemplo o caso em que a empresa manteve as gravações de voz de jovens através do

sistema “*Alexa*” indefinidamente e, utilizou estes dados para fins comerciais, como treinar o seu algoritmo. Um outro evento de utilização de um serviço da *Amazon*, no caso de câmaras de segurança domésticas, conhecido por *Ring*, que incorreu em violações de privacidade dos utilizadores pela falta de rigor nas questões de privacidade e segurança por parte da empresa, o que permitiu que funcionários espiasse ilegalmente os seus clientes (Singer 2023).

A agregação de informação aqui refletida só é possível devido à alargada rede de partilha que existe entre entidades governamentais nos EUA, que se operacionaliza por meio da ferramenta *The Law Enforcement Information Sharing Service (LEIS)*, uma plataforma que permite o intercâmbio de dados e informações baseada em normas. Um regime que permite ao Departamento de Segurança Interna dos EUA e às restantes agências governamentais de *law enforcement* a partilha e permuta rápida e extensiva de informações pertinentes e legalmente partilháveis (Departamento de Segurança Interna dos EUA 2019).

Apesar da missão aqui descrita ser parte integrante de uma ação de controlo da imigração é, no entanto, admitido num dos documentos de proposta contratual oficial de 2014, a oportunidade de monitorização dos próprios cidadãos do país por estas agências e pela plataforma comum no sistema, *ICM*: “*Citizenship can be established a variety of ways to include biographical and biometric system checks. U.S. Citizens are still subject to criminal prosecution and thus are a part of ICM.*” (Imigração e Alfândega dos EUA 2014, 3).

A somar a estas questões tem-se que, no período contratual da plataforma, a administração Trump teve um grande impacto na ação e desenvolvimento do *Investigative Case Management* destas divisões, primariamente da agência *ICE*. Desde a sua entrada formal em 2017, o presidente Donald Trump, garantia a priorização do impacto das leis sobre a imigração, comprometendo-se com uma expansão da ação da divisão *ICE*, agência aqui analisada. De forma a aumentar drasticamente o controlo sobre a imigração, esta administração quis implementar a iniciativa *Extreme Vetting*³, que tem em vista a limitação da imigração ao vetar a entrada a certos grupos, a construção de um muro ao longo da fronteira com o México e, criar uma força de deportação com a aposta nas *ERO*, através de um conjunto de medidas que passaram pelo aumento da vigilância e na exploração de novas ferramentas como os drones de reconhecimento facial e, alargando as bases de dados ao incluir informações biométricas sobre os visitantes e cidadãos americanos (Feeney 2018, 1).

³ Uma iniciativa em que o plano de atuação permitiria à *U.S. Immigration and Customs Enforcement* monitorizar o Twitter, Facebook e outras redes na medida em que auxiliava a agência no assinalar automatizado de pessoas que pretendiam deportar ou a quem pretendiam recusar o visto de entrada, mais voltada para o nicho de muçulmanos. No entanto, logo em 2018, a agência *ICE* confirmou publicamente que a aprendizagem automática da iniciativa seria abandonada, sem informação adicional pormenorizada (Brennan Center for Justice 2017).

A prossecução em força da implementação destas medidas levou a uma atuação corpulenta por parte desta agência e, através de programas como *Secure Communities (SCOMM)*, um programa de partilha de informações entre o *DHS* e o Departamento de Justiça norte-americano, no qual as categorias de imigrantes amovíveis são expandidas; o programa *Section 287 (g)*, do *U.S. Immigration and Nationality Act*, que permite a atribuição de poderes destacados pelo governo federal para a aplicação da lei da imigração e, também, um conjunto de medidas restritivas com vista à limitação das “cidades santuário”, que se libertam de algumas componentes diretivas da imigração, no entanto, estas medidas contribuem para a ameaça ao federalismo e para a abordagem descentralizada que define o policiamento norte-americano (Feeney 2018).

Como referido anteriormente, a plataforma *ICM* tinha em vista apoiar as *HSI*, no entanto, devido a esta premência sobre a imigração é possível ver no documento oficial, *Privacy Impact Assessment for ICE Investigative Case Management*, de 2016, que a força de deportação *ERO* está ligada à monitorização do *ICM*, contribuindo para a ação da *ERO* na deportação de pessoas o que trouxe o descontentamento dos civis e protestos na sede de *Palantir Technologies* pela ajuda que o seu *software* teve na separação de famílias através da deportação de pessoas: “*ERO will also use ICM to query the system for information that supports its civil immigration enforcement cases.*” (Departamento de Segurança Interna dos EUA 2016; Departamento de Segurança Interna 2017). Assim, com o auxílio do **Anexo IX**, repara-se, através de um esquema, na força que a plataforma proporcionada por *Palantir Technologies* tem no aparelho securitário norte-americano pela agregação de informação que lhe é permitida e, pela rede cumulativa e de ligação entre as várias frentes de segurança numa única plataforma privada que, por sua vez, está diretamente inserida no armazenamento de dados possibilitado por outra empresa privada.

Com uma análise dos resultados desta premência sobre a imigração, com a administração Trump, foi possível, até certo ponto, calcular o impacto que plataforma *ICM* teve, a um nível prático, na ajuda a estas agências governamentais:

“No ano fiscal de 2018, a divisão das *HSI* abriu 6 848 investigações no local de trabalho, em comparação com 1 691 no ano fiscal de 2017; iniciou 5 981 auditorias I-9, em comparação com 1 360; e efetuou 779 detenções criminais e 1 525 detenções administrativas relacionadas com o local de trabalho, em comparação com 139 e 172, respetivamente; todas estas categorias

aumentaram 300 a 750 por cento em relação ao ano fiscal anterior.” (Imigração e Alfândega dos EUA 2018)⁶⁴.

Apesar de na administração Biden o apoio a esta agência não ser tão notório, a verdade é que esta divisão continua ativa e a prosseguir com a sua missão e, tal como já foi referido, o contrato entre *Palantir Technologies* e o *DHS*, na providência da plataforma *ICM* às *HSI*, foi renovado por mais cinco anos.

De modo a concluir a análise da última parceria que compõe o estudo de caso, alude-se novamente à missão de *Palantir Technologies*, já referida anteriormente na análise do *United States Securities and Exchange Commission Filing* de 2020, a qual passa por tornar-se o sistema operativo padrão para lidar com dados nos EUA. Esta missão presente nos discursos dos representantes da empresa não representa na sua totalidade e, de forma transparente, as reais capacidades da empresa e em que medida esta se encontra ligada à ação do governo e, por esse motivo, é possível apontar aqui o fenómeno *fallacy of explicit agendas* (falácia de agendas explícitas). O fenómeno indica que existe um secretismo alimentado pelo discurso de um sistema operativo padrão que serve para obscurecer a crescente dependência das entidades governamentais em relação a estas tecnologias de larga escala de vigilância em massa, que também conseguimos analisar ao longo deste estudo de caso (Fleury-Steiner 2019).

É possível, em última análise, reconhecer uma ameaça às liberdades civis pela falta de transparência e supervisão dos dados a que as empresas privadas têm acesso e, por trabalharem diariamente com estes por meio de bases de dados governamentais o que traz uma preocupação acrescida ao identificarmos que existe um estado-padrão associado a esta dinâmica público-privada na condescendência e complacência que se verifica na deferência sem precedentes a um determinismo tecnológico crescente, um “nexo de vigilância Estado-empresas”, devido a estas estratégias discursivas da elite tecnológica quanto à inevitabilidade e excelência na adoção dos seus produtos de software (Fleury-Steiner 2019).

Conclusão

A presente dissertação teve como principal objetivo analisar a cooperação entre o Estado (EUA) e o setor privado (*Palantir Technologies*), mais concretamente a cooperação entre a empresa

⁶⁴ Tradução livre de: In fiscal year 2018, HSI opened 6,848 worksite investigations compared to 1,691 in FY17; initiated 5,981 I-9 audits compared to 1,360; and made 779 criminal and 1,525 administrative worksite-related arrests compared to 139 and 172, respectively; all of these categories surged by 300 to 750 percent over the previous fiscal year.

e o Departamento da Polícia de Los Angeles, o Departamento da Polícia de Nova Orleães e a agência governamental *ICE*, analisadas separadamente, no que diz respeito à vigilância de dados. A cooperação referida compõe o estudo de caso da dissertação, colocando em destaque a conduta da empresa privada, *Palantir Technologies*.

Nesta investigação, a análise foi realizada de modo a compreender-se, por um lado, em que medida esta cooperação se reflete na utilização arbitrária dos dados da população e, por outro, como objetivo secundário, de que forma é que esta cooperação, pressionada pelas competências inerentes às empresas tecnológicas, se reflete numa alteração do papel do Estado sobre o domínio do digital.

Ao contrário do que era pretendido pela sociedade civil e académicos, o Estado não ficou alienado do novo domínio do digital. Especialmente representativa desta linha de pensamento, é a célebre reflexão sobre o ciberespaço, de John Perry Barlow na *Electronic Frontier Foundation* (1996): “Declaro que o espaço social que estamos a construir é naturalmente independente das tiranias que procuram impor-nos. Não tendes o direito moral de nos governar (...).”⁶⁵. Com esta reflexão, o autor reclamava o ciberespaço para a população, numa declaração de independência do ciberespaço, enquanto um domínio da vida social, resolutamente fora do Estado. Na sequência da análise realizada nesta dissertação, concluiu-se que a aspiração em manter o Estado afastado do domínio do digital fracassou, já que, o Estado passou a ter, efetivamente, um papel sobre o domínio digital, marcado pela cooperação com as empresas tecnológicas.

As empresas já tinham acesso garantido ao domínio do digital, uma vez que a sua criação foi facilitada pelas mesmas, no entanto, juntaram-se-lhes os vários Estados. Ficar afastado das comunicações essenciais da população, e o sentimento de perda de controlo e da autoridade sobre um domínio central do espaço comunitário, não fazia parte da agenda do Estado (Deibert 2015, 11).

A atuação dos vários Estados sobre o domínio do digital teve uma maior expressão na sequência dos ataques de 11 de setembro de 2001 ocorridos nos EUA, já que os Estados em geral procuraram garantir a eficácia do seu aparelho de segurança, destacando-se o país afetado.

As transformações nas prioridades do Estado, no período que se seguiu, caracterizaram-se, não só pelo foco nas unidades e agências governamentais securitárias e de *intelligence*, na ajuda

⁶⁵ Tradução livre de: I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us (...).

ao combate ao terrorismo, mas também pela procura do Estado em incluir as mentes do setor privado tecnológico na mesa de negociação política. A recolha de *intelligence*, a análise e visualização de dados, bem como o cálculo do risco de indivíduos, foram o conjunto de competências, inerentes às empresas de software, que conduziram o Estado à cooperação vital com essas mesmas empresas. O pretendido era assegurar a sua própria segurança e mitigar quaisquer riscos. Assim, a cooperação entre as partes, facilitou o trabalho das unidades de segurança do Estado e passou a dar resposta às suas necessidades securitárias.

Partindo para a organização da análise aqui feita, e de forma a responder à pergunta de investigação colocada: “Como se desenvolve a interação do Estado com o setor privado, num contexto de *policing*, em matéria de vigilância e utilização de dados?”, a presente dissertação foi estruturada em três capítulos.

O primeiro capítulo apresentou a abordagem teórica da dissertação, o capitalismo de vigilância, de Shoshana Zuboff (2019). Na análise do capitalismo de vigilância demonstrou-se que foi criada, num determinado contexto internacional, uma adaptação ao capitalismo económico, aplicada ao domínio do digital. A nova versão do capitalismo económico que surgiu dessa adaptação é produto de duas dinâmicas do início do século XXI – o pós-11 de setembro de 2001, que exigiu um investimento acrescido na segurança, e o momento de crise vivido pela empresa tecnológica Google em 2002, provocada pela falta de lucro face aos grandes investimentos da empresa.

Neste período, os EUA eram um país alvejado, que necessitava de aumentar e garantir a sua segurança. A Google encontrava-se num momento de procura de respostas e soluções para as suas necessidades financeiras. Nessa procura, a Google desbloqueou um novo imperativo económico ao descobrir vantagens na utilização do excedente comportamental libertado pelo papel do indivíduo no espaço digital. Observa-se este acontecimento como uma libertação pois, no decurso da utilização da internet, era e continua a ser criado um histórico ou “documento duplicado”, visível e de fácil acesso às empresas, sobre as escolhas, ações, compras e interações realizadas pelos indivíduos (Zuboff 2019).

Ora, foi neste contexto de exploração de oportunidades que a Google acolheu as informações relativas à segunda via da atividade dos indivíduos no domínio digital, tornando-se, assim, esta descoberta, num ponto de viragem, relevante à dissertação. Uma vez encontrada a solução para a crise que atravessava, a recolha dos excedentes tornou-se indispensável para a empresa. Mas não só para a Google. Tornou-se vital para outras empresas que se seguiam, e

também para os Estados. O excedente de dados e informações passou a ser vital e indispensável às empresas na medida em que, a sua utilização e análise passou a permitir-lhes avaliar e prever as escolhas dos utilizadores e ainda, saber qual o conteúdo que lhes deveria ser apresentado no meio digital. Por acréscimo, o excedente de dados passou a responder a interesses alheios de outras empresas que procuravam a certeza na escolha dos utilizadores pelos seus produtos e serviços.

Surgiu assim, neste contexto e com vista a uma maior capitalização, uma nova lógica de acumulação da informação acerca das pessoas, que só foi possível com a vigilância das mesmas nos corredores digitais. Além da acumulação de dados, as empresas encurralaram os mesmos, através de interfaces de programação de aplicações⁶⁶, com funções semelhantes aos interfaces referidos com a plataforma *ICM* na parceria com as *HSI*.

Ora, os EUA viram na capitalização de dados, proporcionada pelas empresas, uma oportunidade para colmatar as questões securitárias que atravessavam no imediato ao 11 de setembro. Tendo em conta esta realidade excecional que se vivia, os EUA encontraram nas empresas tecnológicas privadas, o escape extraordinário para a vigilância massificada da população. As empresas ofereciam um leque de dados, aos quais os Estados não tinham acesso anteriormente, e proporcionavam uma contextualização do conjunto de dados, na forma de análises preditivas do cálculo do risco da população, considerando o foco determinante no combate ao terrorismo.

No segundo capítulo desta dissertação é feito um afunilamento na investigação, introduzindo a conjuntura que proporcionou tanto a colaboração entre a empresa *Palantir Technologies* e os EUA, como o avanço da abordagem *intelligence-led policing*. Após iniciar o capítulo com uma visão e caracterização geral acerca da empresa *Palantir Technologies*, a análise progrediu mediante o fio condutor que levou à evolução das características da vigilância de dados, por parte do Estado e das empresas. O início da análise corresponde ao período após o 11 de setembro de 2001, com a introdução de diretivas extraordinárias, que iriam circunscrever o desenvolvimento das parcerias analisadas nesta dissertação. No entanto, estas diretivas tenderam a prolongar-se após o período de crise, registando-se uma propagação e intensificação da vigilância de dados dos indivíduos (Véliz 2020), como se refere no terceiro capítulo da dissertação.

⁶⁶Interfaces de programação de aplicações são uma ferramenta intermediária entre uma aplicação e o servidor *Web*, onde se processa a transferência de dados entre sistemas. Trata-se de um conjunto de regras que permitem às aplicações comunicarem entre si através de uma série de normas e protocolos (MuleSoft s.d.)

Duas das diretivas introduzidas pelo Estado são de importância tal, que se faz crucial referi-las. Essas diretivas são, a diretiva *Homeland Security Act* e a diretiva *Smart Policing Initiative*. Ambas foram estabelecidas em estreita cooperação com o setor privado, ambas atribuíram um conjunto de fundos às unidades de segurança nacional e ambas foram criadas de modo a possibilitar a análise preemptiva de riscos à segurança nacional. No entanto, a primeira permitia a agregação de dados e a sua transferência pelas agências, enquanto a segunda incentivava, em especial os departamentos de *law enforcement*, a apostar na adoção de metodologias baseadas em dados.

A análise e atuação preemptiva de todas as unidades de segurança dos EUA desenvolveu-se com o reconhecimento e valorização do conceito de *intelligence*, que de forma sucinta é um processo que envolve a contextualização de dados e o cálculo do risco para que seja possível a preempção de ameaças.

No terceiro capítulo, desenvolveu-se uma análise pormenorizada da cooperação entre a empresa *Palantir Technologies* e os EUA, ao optar por uma metodologia qualitativa e pela escolha de um estudo de caso ilustrativo. Com o objetivo de aplicar a abordagem teórica do capitalismo de vigilância de Shoshana Zuboff (2019), foi feita uma análise substantiva de três parcerias entre a empresa *Palantir Technologies* e diferentes unidades de segurança do Estado em questão. Foi investigada, em primeiro lugar, a cooperação entre a empresa e o Departamento da Polícia de Los Angeles, no contexto da operação *LASER*; em segundo lugar, a cooperação entre a empresa e o Departamento da Polícia de Nova Orleães, no contexto do programa *NOLA For Life*; e em terceiro lugar, a cooperação entre a empresa e a agência governamental *ICE* dos EUA, mediante a disponibilização da plataforma *ICM*, por parte da empresa. Demonstrou-se, neste terceiro capítulo, que a vigilância foi facilitada pelas capacidades analíticas da empresa *Palantir Technologies*, que por acréscimo, conseguiu ter acesso aos dados institucionais sem uma supervisão adequada.

Finda a descrição da estrutura desta dissertação, apresenta-se de seguida as conclusões obtidas a partir da mesma, relativamente às implicações de uma cooperação entre o Estado e o setor privado, num contexto de *policing*, em matéria de vigilância de dados.

Em primeiro lugar, concluiu-se que não existia e continua a não existir uma entidade reguladora, adaptada, especialista em controlo de vigilância de dados, capaz de dar resposta às exigências de uma supervisão às empresas, de calibre tecnológico como o da empresa *Palantir Technologies*. Logo de seguida, e como consequência dessa falta de uma entidade reguladora, verificou-se uma tendência para o comprometimento dos direitos à privacidade e proteção de

dados da população, com a incapacidade de assegurar a proteção desses mesmos direitos. Este comprometimento deve-se ao fenómeno de transição em massa de informação sobre a população para uma terceira entidade, sem que haja um reconhecimento detalhado e divulgado ao público, do uso e destino que é dado aos seus dados. Estas falhas na informação ao público, devem-se ao carácter sigiloso que circunscreve estas parcerias.

Em segundo lugar, aludindo ao capitalismo de vigilância, concluiu-se que se verificaram ainda outras implicações na vida dos indivíduos, devido à cooperação entre o Estado e as empresas, e devido à adoção e utilização de metodologias baseadas em dados. Ou seja, a utilização de dados enviesados, como consequência dos resultados apresentados pelas análises algorítmicas, provocou implicações ao nível do quotidiano dos indivíduos. Percebeu-se que, o historial (informações) dos Departamentos da Polícia, nomeadamente aquele que diz respeito a práticas institucionais associadas à discriminação racial, corre o risco de ser incorporado de forma instantânea nas análises das plataformas tecnológicas, aquando do cálculo do risco dos indivíduos, o que acarreta implicações, como o comprometimento na eficácia destes métodos e o possível aumento do risco de propagação do viés e da parcialidade. Verificou-se e comprovou-se que, com a análise da operação *LASER* e do programa *NOLA For Life*, existiu uma falta de clareza em questões de imparcialidade.

Estas conclusões foram obtidas uma vez que a incidência do *policing*, por parte dos Departamentos da Polícia, continuou a ser realizado sobre o mesmo grupo de pessoas que atingia antes da utilização dos produtos da empresa *Palantir Technologies*: hispânicos/latinos e negros/afro-americanos, jovens afro-americanos, essencialmente do género masculino, com baixa escolaridade e subempregados (Stop LAPD Spying Coalition 2021; Schirmer e Asher 2014). Concluiu-se ainda que a eficiência da adoção de métodos baseados em dados foi questionada, por parte da sociedade civil, após as avaliações realizadas à cooperação entre os Departamentos da Polícia e a empresa *Palantir Technologies* terem demonstrado a inexistência de uma comprovação na ligação direta entre a introdução destas tecnologias e os resultados na redução do crime.

Em terceiro e último lugar, concluiu-se que existem outras implicações da cooperação entre o Estado e as empresas, e da adoção das metodologias já referidas. Algumas dessas implicações são a vigilância massificada dos dados dos indivíduos, que passa a ser realizada por defeito, dando origem à instituição de um estado-padrão; após a realização da avaliação do risco dos indivíduos, por parte da empresa, é feita uma classificação da população; e a propagação dos

dados no sistema que passou a ser irreversível. Assim, as consequências destas implicações podem ser devastadoras, já que, uma vez introduzidos os dados nos sistemas computacionais, não é possível reverter o processo de propagação, havendo o risco desses dados serem utilizados para outros propósitos, que servem outros interesses e agendas, tanto do setor privado, como do próprio Estado, criando-se um ciclo com efeito “bola de neve”.

Estas implicações prosperam com a evolução das tecnologias e dos métodos de processamento de dados. Mesmo que uma certa empresa assegure a proteção de dados, a sua utilização de produtos externos de outras empresas que ajudam no processamento desses mesmos dados, indica que existe a possibilidade de a proteção dos dados pessoais não estar a ser garantida, uma vez que as políticas de privacidade das empresas podem não convergir. Exemplo disto, é o caso da empresa aqui analisada, *Palantir Technologies*, com a sua utilização dos Amazon *Web Services* (serviços de alojamento de dados em nuvem, disponibilizados pela empresa Amazon). A presente análise permitiu concluir que existe uma dicotomia entre as obrigações e as expectativas na garantia dos mesmos códigos de conduta ao nível da privacidade de dados, o que não reflete a transparência desejada.

Estas questões e formas de atuação associadas às tecnologias, podem ainda levar a uma dissuasão na prática da liberdade de expressão, na medida em que existe um receio, crescente nos indivíduos, de serem identificados como potenciais riscos perante as análises dos sistemas computacionais das empresas (Stanley 2016).

Em jeito conclusivo, e respondendo à pergunta de investigação colocada no início desta dissertação – “Como se desenvolve a interação do Estado com o setor privado, num contexto de *policing*, em matéria de vigilância e utilização de dados?” – a cooperação entre o Estado e o setor privado, na vigilância dos dados da população desenvolveu-se num contexto de instabilidade, nomeadamente no contexto do pós-11 de setembro, em que foram aprovadas medidas extraordinárias de segurança. As medidas incluem a agregação excecional de dados, de forma livre e inteligível pelas empresas privadas, perante a declaração de uma Guerra ao Terror, e incluem ainda a primazia do combate ao terrorismo na política interna e externa dos EUA. Com estes objetivos, o Estado teve necessidade de contratar empresas como a empresa *Palantir Technologies* para facilitar a recolha, acumulação e análise dos dados, de modo a fazer alterações nos processos de tomada de decisão. Ainda que, indubitavelmente, exista um grau reconhecido de eficiência nesta cooperação, a mesma não transpõe os limites de uma regulamentação à

vigilância de dados, na medida em que, não havendo acesso nem escrutínio públicos sobre o uso e o destino dos dados, compromete-se a privacidade e proteção dos dados dos indivíduos.

A partir da análise das três cooperações estabelecidas entre o Estado e a empresa, verificou-se que uma se mantém ativa (a estabelecida entre a empresa *Palantir Technologies* e a *HSI*, divisão da agência governamental *ICE*, com a utilização contínua da plataforma *ICM*. No entanto, as outras parcerias aqui analisadas foram encerradas após uma investigação à sua eficácia. A continuidade de alguns dos contratos assinados, como é o caso da referida acima, deveu-se a vários fatores, entre eles, a assinatura dos contratos no sigilo, a impossibilidade de um conhecimento holístico sobre as reais capacidades analíticas das empresas, sobre as estratégias e sobre os métodos utilizados, orientados por dados, e o tráfico de influências entre o Estado e o setor privado, proporcionado pela fraca regulamentação sobre a proteção de dados. Estes fatores permitiram, e permitem ainda, ao Estado, manter uma capitalização da informação acerca da sua população.

A análise realizada permite identificar algumas avenidas de pesquisa futura. Uma das vias possíveis será efetuar o exercício de análise de um método comparativo entre parcerias, tentando perceber se e para quais dessas parcerias de alguma forma se justificaria, ou não, uma vigilância massificada de dados, tendo em conta questões de segurança nacional. Outra via possível e interessante será estudar a evolução da regulamentação de proteção de dados nos EUA, de forma a perceber que oscilações ocorrem nessa mesma regulamentação, em diferentes momentos da sua relação com a número um neste campo, a União Europeia. Isto é, analisar a regulamentação de proteção de dados nos EUA, tendo em conta as normas estabelecidas nos diferentes acordos de transferência de dados, celebrados entre os EUA e a União Europeia. Desses acordos, que preveem um mecanismo jurídico para as empresas transferirem dados pessoais da União Europeia para os EUA, temos o *Safe Harbor* e o *Privacy Shield* que foram substituídos pelo atual enquadramento *Data Privacy Framework*.

Tabelas.

Tabela 1. Objetivos declarados versus a ação dos departamentos de Los Angeles e Nova Orleães: assegurar a segurança pública com novas ferramentas de *predictive policing*. (Criação livre da autora).

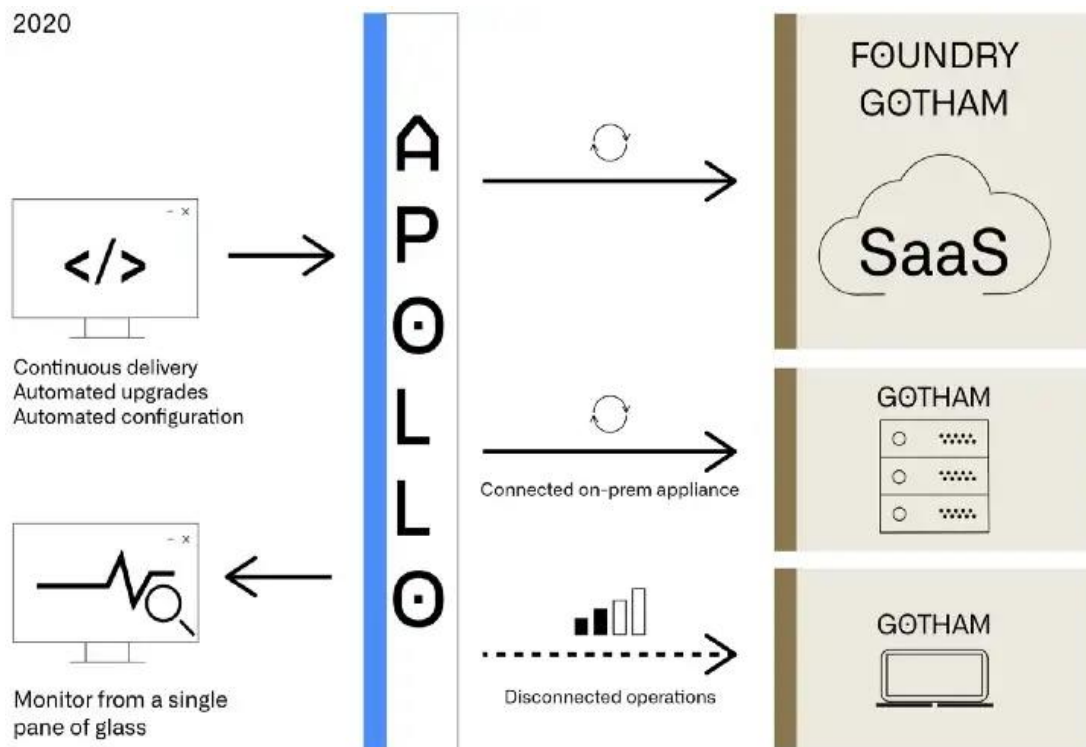
Objetivos declarados	Ação dos departamentos referidos
Segurança pública	Práticas inconstitucionais; Litígios com a comunidade
Conduta imparcial	Decretos de consentimento de forma a reduzir o viés racial
Vigilância defensiva	Vigilância em massa
Responsabilidade e transparência	Ausência de responsabilização e transparência
Supervisão	Uma autoridade estatutária inexistente e uma ausência de mecanismos de controle
Avaliação e gestão do risco	Classificação e triagem social: <i>social sorting</i>
<i>Predictive policing</i> : utilização de <i>raw data</i>	Resultados enviesados: utilização de <i>dirty data</i>
Estratégias baseadas em dados, para ajudar no processo de tomada de decisão	dados servem como verificação da intuição
Exemplo: “Mission: Work with community and agency partners to develop and implement a comprehensive strategy that reduces murder in the City of New Orleans by employing targeted prevention, intervention, enforcement and rehabilitation initiatives” (City of New Orleans 2013, 38).	Falta de evidência na eficiência destas parcerias e destes novos produtos de <i>predictive policing</i> na redução da taxa de criminalidade e no combate ao viés dos departamentos.

**Tabela 2. Categorias de análise do Capitalismo de Vigilância de Shoshana Zuboff.
(Criação livre da autora).**

O que é	Leis de movimento	Imperativos categóricos	Metodologias de secretismo/sigilo	Poder 'instrumentarista'
• Uma nova ordem económica institucional que resulta de um ciclo de reinvestimento no excedente comportamental; • Uma economia de vigilância guiada por uma lógica de acumulação; • O capitalismo de vigilância não é a tecnologia, é a forma de mercado que os atores dão sentido pelas lógicas sociais e económicas operantes; • O uso da tecnologia como expressão dos objetivos económicos; • Uma forma de mercado que sobrevive pelo meio digital, mas que consegue operar no mundo real.	• Leis já conhecidas do capitalismo como: a produção competitiva, a maximização do lucro, a produtividade e crescimento; • Para além das já estabelecidas características inerentes ao capitalismo que conhecemos juntam-se agora novos imperativos que operam através dos mecanismos próprios desta nova forma de mercado que tem as suas leis de movimento <i>sui generis</i>.	• O imperativo de extração e as economias de escala; • O imperativo de predição e as economias de âmbito; • O imperativo de predição e as economias de ação.	• Estas metodologias levaram ao sucesso da ação dos capitalistas de vigilância: • O ineditismo; • As declarações da agenda com a utilização de eufemismos; • Contexto histórico; • Fortificações através de afinidades eletivas com o estado; • Ciclo de expropriação; • Dependência, fecho de alternativas e a persuasão social; • Interesse legítimo; • A inevitabilidade e rapidez; • Interesse próprio; • A inclusão, identificação e autoridade; • A ideologia sobre a fragueza humana.	• 'Instrumentação' com a arquitetura tecnológica omnipresente • + • 'Instrumentalização' refere-se à próxima observação das relações sociais que caracterizam a experiência humana de modo que as consigam tornar uma mercadoria no ciclo preditivo.

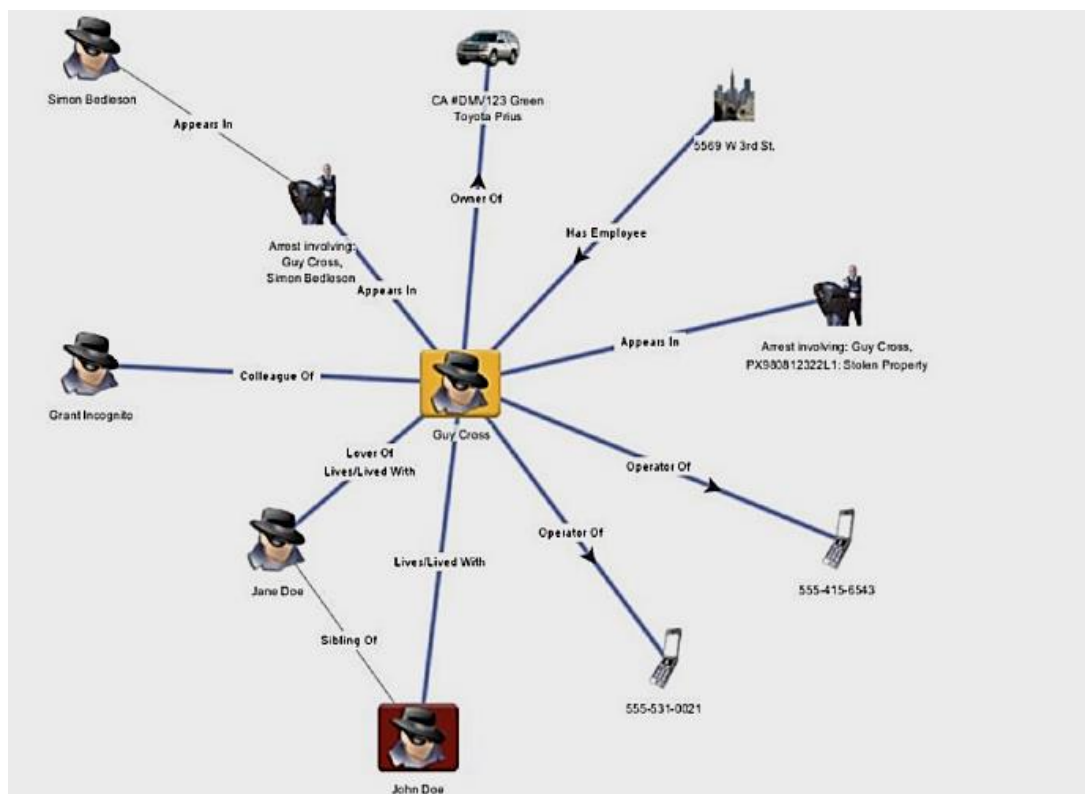
Anexos

Anexo I - Software enquanto serviço – produto *Apollo* de *Palantir Technologies*



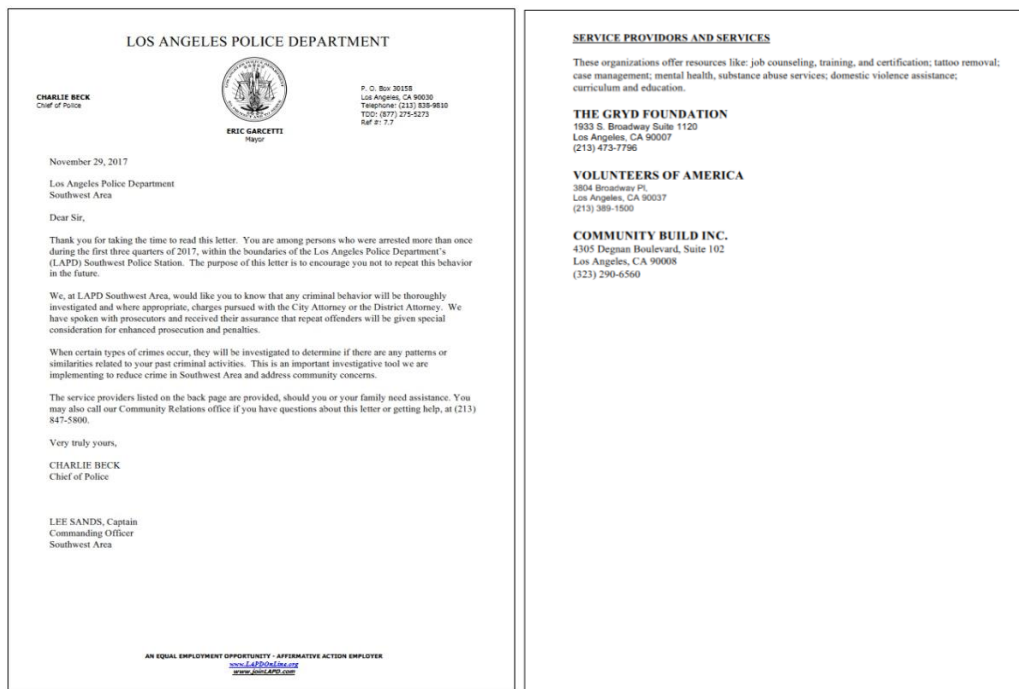
Fonte: Palantir Technologies. 2020. "Palantir Apollo: Powering SaaS where no SaaS has gone before." *Medium*. Publicado a 29 de setembro de 2020. Acedido a 26 de abril de 2023. <https://blog.palantir.com/palantir-apollo-powering-saas-where-no-saas-has-gone-before-7be3e565c379>.

Anexo II - Rede de contactos estabelecida e visualizada através do software de Palantir Technologies



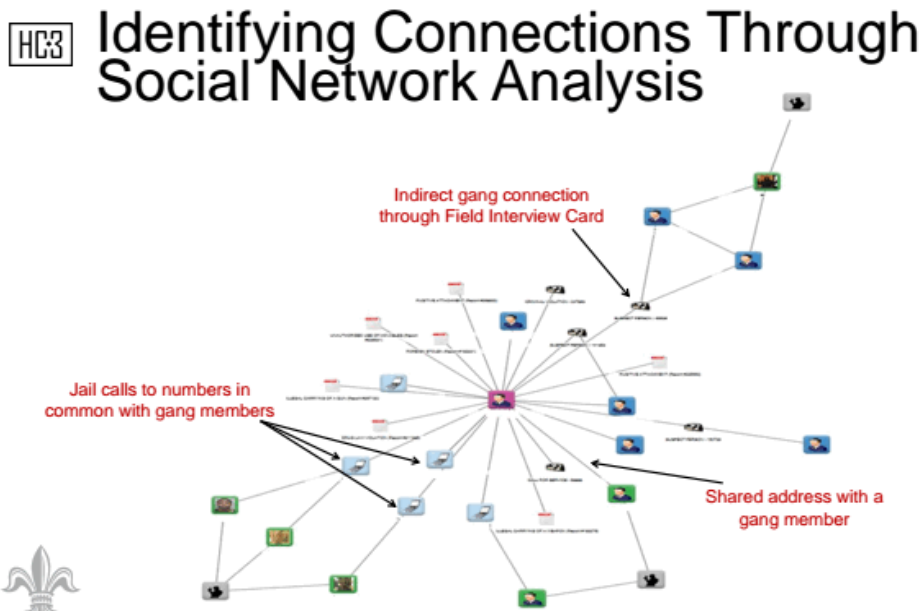
Fonte: Brayne, Sarah. 2017. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82 (5): 977-1008.

Anexo III – Exemplo de uma carta enviada a um infrator reincidente



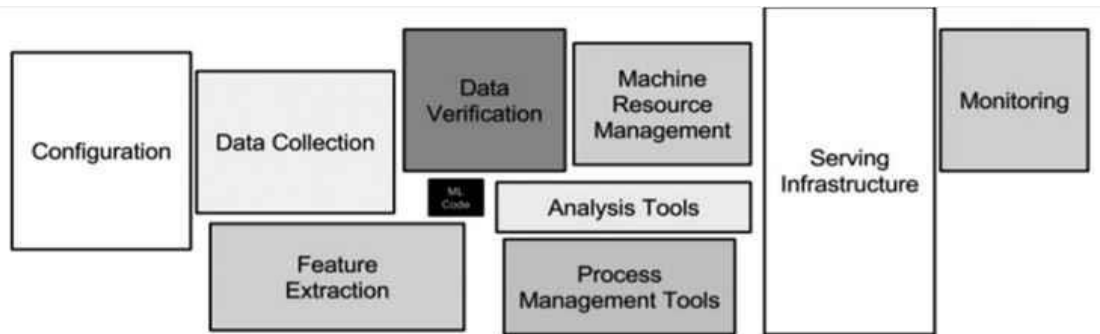
Fonte: Office of the Inspector General. 2019. *Review of Selected Los Angeles Police Department Data-Driven Policing Strategies*. Los Angeles Police Commission: Office of the Inspector General. http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.

Anexo IV – Utilização da estratégia: análise de redes/interações sociais



Fonte: Schirmer, Sarah, e Jeff Asher. 2014. "HOBBITCON ° 3." Documento interno. DocumentCloud. Acedido a 18 de outubro de 2023. Arquivado em <https://www.documentcloud.org/documents/4344815-Nola-hc3-Final->

Anexo V – A “caixa-negra” nos sistemas de aprendizagem automática



Fonte: Iliadis, Andrew, e Amelia Acker. 2022. “The Seer and the Seen: Surveying Palantir’s Surveillance Platform.” *The Information Society* 38 (5): 334-363.

Anexo VI – Relação contratual entre Palantir Technologies e a agência ICE

08/09/23, 16:58 FPDS-NG : ICDUSER [IDV Print]

Print Close Help

Transaction Information
 IDV Type: Other IDC
 IDV Status: Final
 Closed Status: Yes
 Prepared Date: 09/19/2014 14:56:27
 Last Modified Date: 08/04/2022 08:31:01
 Closed Status Date: 08/04/2022 08:31:01
 Approved Date: 09/26/2014 15:02:18
 Prepared User: BETHANY.STUTLER@DHS.GOV
 Last Modified User: MISTY.WEINHOLD@ICE.DHS.GOV
 Closed By: MISTY.WEINHOLD@ICE.DHS.GOV
 Approved By: BETHANY.STUTLER@DHS.GOV

Document Information
 Agency: 7012
 Procurement Identifier: HSCETC14C00002
 Modification No: 0
 IDV ID: 7012
 Referenced IDV ID: 7012
 Reason For Modification: HSCETC-14-R-00002
 Solicitation ID: HSCETC-14-R-00002
 Agency Main Sub Identifier Account Account Initiative
 Treasury Account Symbol: 70 0543
 Dates
 Date Signed: 09/25/2014
 Period of Performance Start Date: 09/26/2014
 Last Date to Order: 09/25/2019
 Amounts
 Action Obligation: \$12,472,821.20
 Base and All Options Value (Total Contract Value): \$41,629,069.08

Purchaser Information
 Contracting Office Agency ID: 7012
 Contracting Office ID: 70CTDO
 Funding Agency ID: 7012
 Funding Office ID: CIOPEO
 Foreign Funding: Not Applicable
 Contracting Office Agency Name: U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
 Contracting Office Name: INFORMATION TECHNOLOGY DIVISION
 Funding Agency Name: U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
 Funding Office Name: OFFICE OF THE CHIEF INFORMATION OFFICE

Entity Information
 FAR 4.1102 Exception: Remove Exception
 Unique Entity ID: HNN4F9JZWDY8
 Legal Business Name: PALANTIR USG, INC.
 DBAN: PALANTIR USG, INC.
 Street: 635 WAVERLEY ST
 Street2: PALO ALTO
 City: CA
 State: CA
 Zip: 943010000
 Country: UNITED STATES
 Phone: (650) 815-0200
 Fax No: (650) 618-2298
 Congressional District: Show Details

Business Category
 Organization Type: CORPORATE NOT TAX EX
 State of Incorporation: DE
 Country of Incorporation: USA
 Business Types
 Corporate Entity, Not Tax Exempt
 Relationship With Federal Government
 All Awards
 Organization Factors
 For Profit Organization

Contract Data
 Type of Contract: Firm Fixed Price
 Inherently Governmental Functions: CT
 Major Program: Indefinite Delivery / Requirements
 National Interest Action: None
 Type of IDC: Single Award
 Multiple Or Single Award IDV: No
 Program Acronym: Not Applicable exempt from CAS
 Cost Accounting Standards Clause: No
 Consolidated Contract: No
 Undefined Action: Yes
 Multiyear Contract: Yes - Service where PBA is used.
 Performance Based Service Acquisition: Not Applicable
 Contingency Humanitarian Peacekeeping Operation: Not Applicable
 Legislative Mandates: Inter Agency Contracting Authority

<https://www.fpds.gov/DataCollection/contracts/jsp/IdvBaseController.jsp?undefined=undefined>

1/2

08/09/23, 16:58 FPDS-NG : ICDUSER [IDV Print]

Clinger-Cohen Act: No
Service Contract Act: Not Applicable
Walsh-Healey Act: Not Applicable
Davis Bacon Act: Not Applicable
Interagency Contracting Authority: Not Applicable
Other Interagency Contracting Statutory Authority: (1000 characters)
Contract Marketing Data
 Website URL: (https://www.fpds.gov)
 Who Can Use: Only the Agency awarding the contract may place orders.
 FIPS 95 codes / Other Text:
 Email Contact:
 Individual Order / Call Limit: \$0.00
 Fee for Use of Service: Fixed
 Varies by Amount
 Varies by Other Factor
 No Fee
 Lower Value Upper Value
Ordering Procedure: (Optional if Website URL is provided, otherwise mandatory)
Product Or Service Information
 Product/Service Code: D307 Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
 Principal NAICS Code: 541512 Description: COMPUTER SYSTEMS DESIGN SERVICES
 Claimant Program Code:
 Bundled Contract: Not a bundled requirement
 GFP Provided Under This Action: Transaction does not use GFP.
 Recovered Materials/Sustainability: No Clauses Included and No Sustainability Included OMB Policy on Sustainable Acquisition
 Domestic or Foreign Entity: U.S. Owned Business
 Sea Transportation: Select One
 Description Of Contract Requirement: (4000 characters)
 ICE COTS based, web-enabled Investigative Case Management (ICM) System for ICE TECS MOD Program Office.
Competition Information
 Extent Competed For Referenced IDV:
 Extent Competed: Full and Open Competition
 Solicitation Procedures: Negotiated Proposal/Quote
 Type Of Set Aside: No set aside used.
 Evaluated Preference: No Preference used
 SBIR/STTR: Select One
 Fair Opportunity/Limited Sources: Select One
 Other Than Full And Open Competition: Commercial Products and Services Acquisition Procedures:
 A7B Action: No
 Contract Opportunities Notice: Yes
 Local Area Set Aside: No
 Number Of Offers Received: 7
 Small Business Competitiveness Demonstration Program: No
 Commercial Item Test Program:
 Preference Programs / Other Data
 Contracting Officer's Business Size Selection: Other than Small Business
 Subcontract Plan: Plan Required - Incentive Not Included

<https://www.fpds.gov/DataCollection/contracts/jsp/IdvBaseController.jsp?undefined=undefined>

2/2

Fonte: Federal Procurement Data System. 2014. "ICE COTS based, web-enabled Investigative Case Management (ICM) System for ICE TECS MOD Program Office." Acedido a 21 de agosto de 2023.

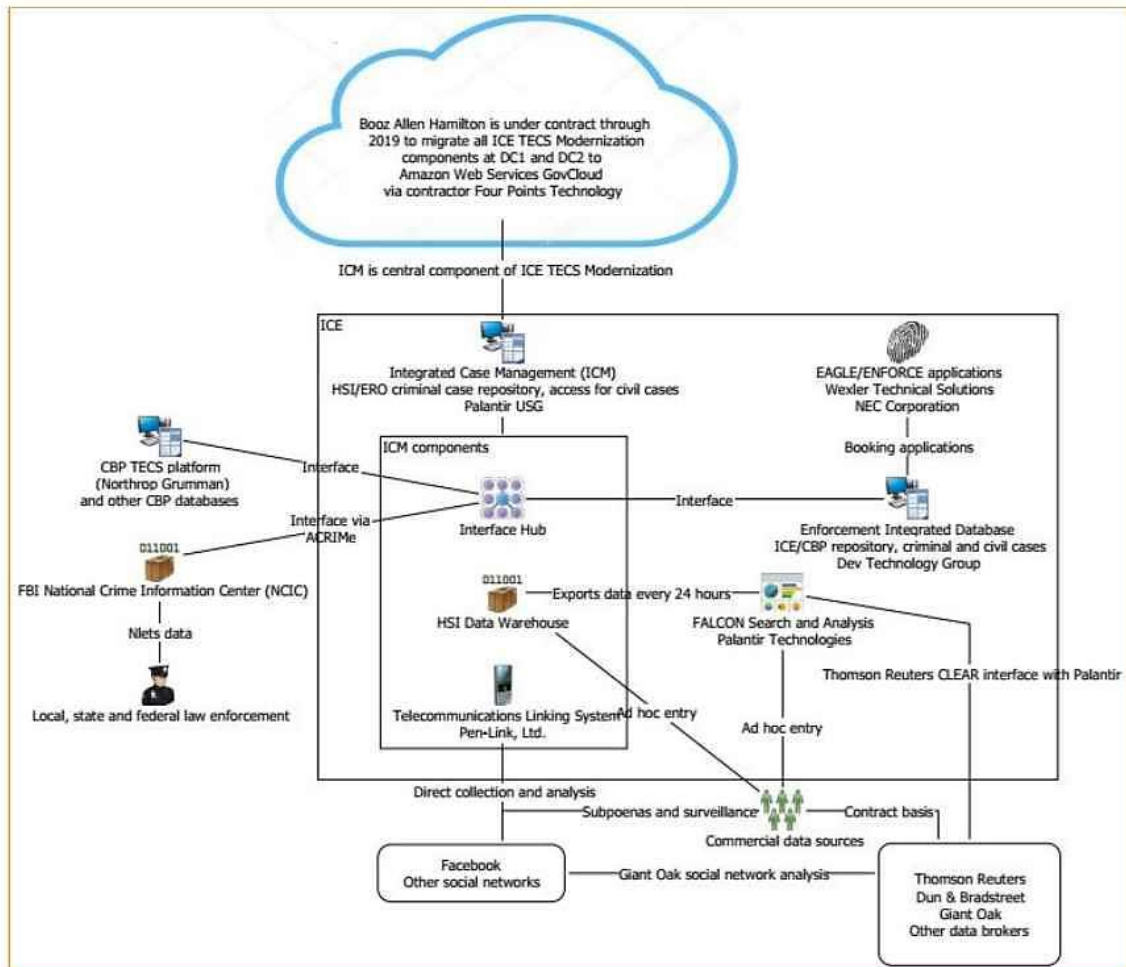
<https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPD.S.GOV&q=Palantir+ICE>.

Anexo VII –Bases de dados a que é possível aceder a partir da plataforma ICM

Database	Information Accessible	Agency/ Sub-agency
ATS (Automated Targeting System)	ICM users may query ATS from within ICM for information on passengers, vehicle or aircraft border crossings, secondary investigation logs, visa and passport data, and other information relevant to investigations and manually copy any pertinent data into subject records or case documents.	DHS/CBP
EID (Enforcement Integrated Database)	ICM users may access EID arrest data. EID arrests are primarily made by HSI or ERO. Within ICM, a user may query EID for an individual and if that individual's record is found, the user can pull all information collected on that individual contained in EID into ICM.	DHS/ICE
FALCON-DARTTS (FALCON Data Analysis & Research for Trade Transparency System)	ICM can search FALCON-DARTTS from within the ICM application. FALCON-DARTTS contains information on Financial Crimes Enforcement Network data, currency and monetary instrument reports, currency transaction reports, suspicious activity reports, reports relating to coins and currency received in nonfinancial trade or business, reports of foreign bank, and financial accounts.	DHS/ICE
NCIC (National Crime Information Center)	ICM users may query NCIC from within ICM via ICE's existing connection to NCIC. This connection is housed within ICE's Alien Criminal Response Information System (ACRIME). NCIC contains information on criminal targets, immigration violators, stolen articles, warrants, terrorist watchlist records, state and federal criminal history reports, and reports of missing persons.	DOJ/FBI
SEACATS (Seized Assets and Cases Tracking System)	ICM users may query SEACATS from within ICM to obtain records of seizures of contraband. This usually occurs when an ICM user is creating a seizure report within a case. The user can directly import the data from SEACATS into the seizure report. Information from SEACATS may also be manually input into other case documents, such as ROIs or arrest reports.	DHS/CBP
SEVIS (Student and Exchange Visitor Information System)	ICM users may search SEVIS from within ICM and either directly import or manually copy SEVIS data into a case record. SEVIS contains biographic and immigration status data about individuals who are temporarily admitted to the United States as students or exchange visitors.	DHS/ICE
TECS (Treasury Enforcement Communications System)	ICM users may query TECS from within ICM for information related to any person associated with a case. This includes subject records, border crossings, and inspection records. TECS is the legacy case management system used by CBP; use of TECS was scheduled to end by September 30, 2015.	DHS/CBP

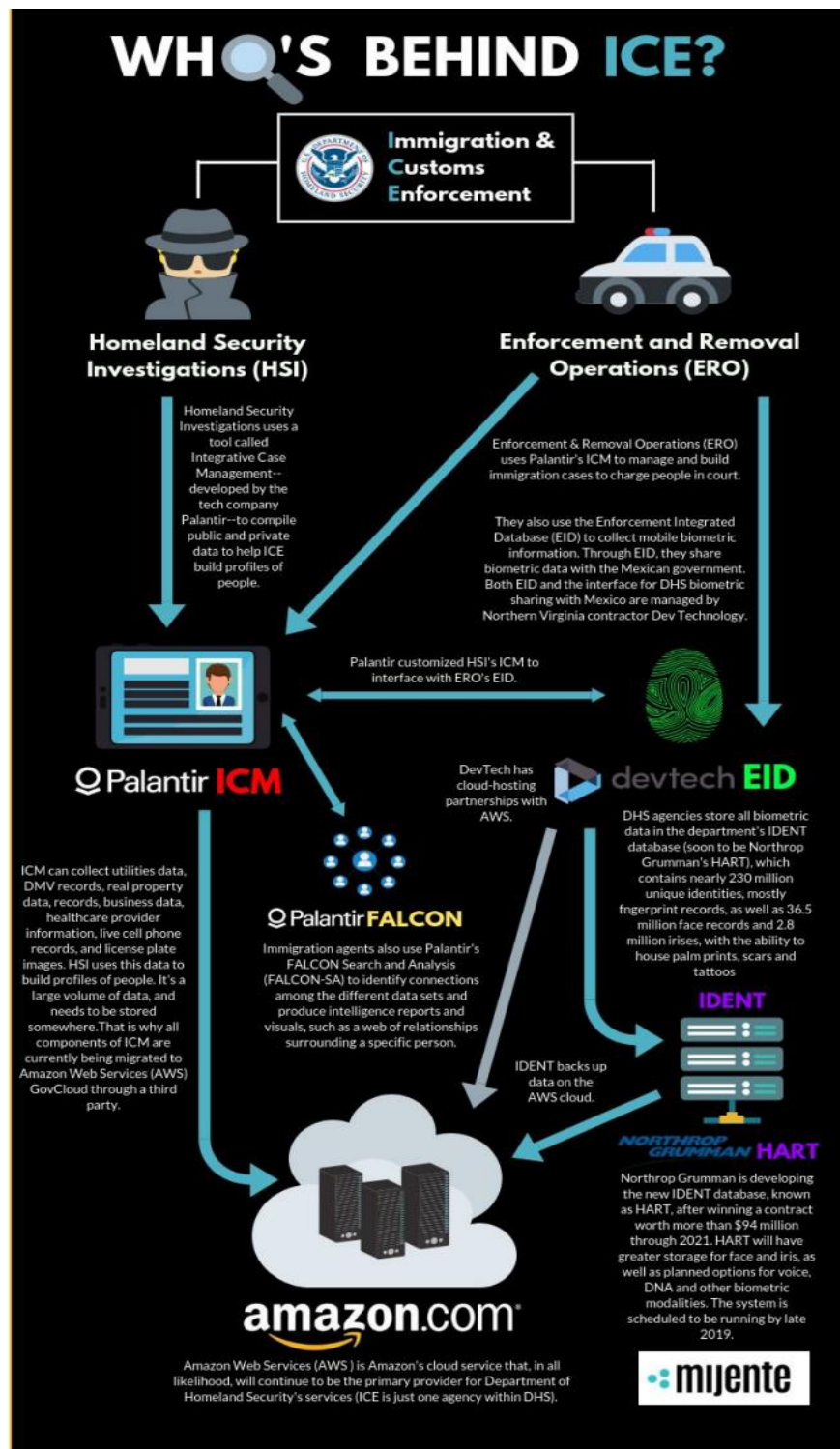
Fonte: Knight, Emma, e Alex Gekker. 2020. "Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures." *Surveillance & Society* 18 (2):231-243.

Anexo VIII – Os sistemas de gestão de processos da agência ICE e a sua rede contratual



Fonte: Mijente. 2018. *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*.

Anexo IX – Rede de elementos que sustentam a atividade da agência ICE



Fonte: Mijente. 2018. *Who's Behind ICE? The Tech and Data Companies Fueling Deportations.*

BIBLIOGRAFIA:

Entrevista:

Entrevista realizada a um representante da empresa *Palantir Technologies*. 2023. Entrevistado pela autora da dissertação. Online [via Microsoft Teams]. 24 de maio de 2023.

Fontes Primárias:

Bureau of Justice Assistance. 2013. *Smart Policing Initiative Data. Analysis. Solutions*. United States Department of Justice. <http://bjaojp.gov/sites/g/files/xyckuh186/files/Publications/SmartPolicingFS.pdf>.

City of New Orleans. 2013. *NOLA For Life. Comprehensive Murder Reduction Strategy*. Acedido a 18 de outubro de 2023. https://www.nola.gov/nola/media/Mayor-s-Office/Files/NOLA%20FOR%20LIFE/NOLA-FOR-LIFE-Sept2013-book-pdf_1.pdf.

Departamento de Justiça dos EUA. 2011. *Investigation of the New Orleans Police Department*. U.S. Department of Justice Civil Rights Division. https://www.justice.gov/sites/default/files/crt/legacy/2011/03/17/nopd_report.pdf.

Departamento de Justiça dos EUA. S.d. *Office of Community Oriented Policing Services*. Office of Community Oriented Policing Services. <https://www.justice.gov/doj/office-community-oriented-policing-services>.

Departamento de Segurança Interna dos EUA. 2002. *Homeland Security Act of 2002, Public Law 107-296*. Senate and House of Representatives of the United States of America in Congress. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

Departamento de Segurança Interna dos EUA. 2010. *IT Program Assessment: CBP & ICE – Traveler Enforcement Compliance Systems (TECS) Modernization (2010)*. <https://www.dhs.gov/xlibrary/assets/mgmt/itpa-cbp-tecsmod2010.pdf>.

Departamento de Segurança Interna dos EUA. 2016. *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045*. Homeland Security. <https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf>.

Departamento de Segurança Interna dos EUA. 2017. *Unaccompanied Alien Children Human Smuggling Disruption Initiative. Concept of Operations*. Homeland Security. Acedido a 12 de janeiro de 2024. Arquivado em <https://s3.documentcloud.org/documents/5980596/Smuggling-Initiative-ConOP.pdf>.

Departamento de Segurança Interna dos EUA. 2019. *Privacy Impact Assessment for the Law Enforcement Information Sharing Service (LEIS Service). DHS/ICE/PIA-051*. Homeland Security. Última atualização a 31 de março de 2023. <https://www.dhs.gov/publication/dhsicepia-051-law-enforcement-information-sharing-service-leis-service>.

Departamento de Segurança Interna dos EUA. S.d. “DHS Law Enforcement.” Homeland Security. Última atualização a 27 de abril de 2023. Acedido a 20 de outubro de 2023.

- <https://www.dhs.gov/dhs-law-enforcement>.
- Departamento de Segurança Interna dos EUA. S.db. “Law Enforcement.” Homeland Security. Última atualização a 11 de junho de 2024. Acedido a 7 de maio de 2023. <https://www.dhs.gov/topics/law-enforcement>.
- Federal Procurement Data System. 2014. “ICE COTS based, web-enabled Investigative Case Management (ICM) System for ICE TECS MOD Program Office.” Acedido a 21 de agosto de 2023. <https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=Palantir+ICE>.
- Federal Procurement Data System. 2021. “Palantir US Government Contracts Corpus.” Acedido a 21 de agosto de 2023. <https://scholarshare.temple.edu/bitstream/handle/20.500.12613/6805/PalantirUSGovContractsCorpus.pdf?sequence=4&isAllowed=y>.
- Federal Procurement Data System. S.d. Procura por “Lista de contratos mais recentes, 2022-2023: Palantir.” Acedido a 21 de agosto de 2023. <https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir+2023&renderer=jsp&length=130>.
- Federal Procurement Data System. S.d. Procura por “Palantir.” Acedido a 21 de agosto de 2023. <https://www.fpds.gov/ezsearch/search.do?s=FPDS.GOV&indexName=awardfull&templateName=PDF&q=Palantir&renderer=jsp&length=1274>.
- Google Inc. 2003. Generating User Information For Use in Targeted Advertising. US Patent 9, 235, 849 B2, submetida a 31 de dezembro de 2003, e emitada a 12 de janeiro de 2016. <https://patentimages.storage.googleapis.com/95/87/69/1b3a80e964f76c/US9235849.pdf>.
- HigherGov. 2014. HSCETC-14-R-00002-STEP 1 Questions and Responses. Immigration and Customs Enforcement. <https://www.highergov.com/document/hscetc-14-r-00002-step-1-questions-and-responses-updated-pdf-fa2282/>.
- Imigração e Alfândega dos EUA. 2014. *Immigration and Customs Enforcement (ICE) TECS Investigative Case Management (ICM) Statement of Objectives*. Homeland Security. <https://s3.documentcloud.org/documents/3478481/ICE-ICM-Statement-of-Objectives.pdf>.
- Imigração e Alfândega dos EUA. 2018. “ICE worksite enforcement investigations in FY18 surge.” Última atualização a 11 de dezembro de 2018. Acedido a 12 de janeiro de 2024. <https://www.ice.gov/news/releases/ice-worksite-enforcement-investigations-fy18-surge>.
- Imigração e Alfândega dos EUA. 2023. “ICE TECS Modernization Industry Day – June 20, 2023.” YouTube, 49:55. https://www.youtube.com/watch?v=nvgE_ivZ7dA.
- Imigração e Alfândega dos EUA. S.d. “Immigration Enforcement; Combating Transnational Crime.” U.S. Immigration and Customs Enforcement (ICE). Última atualização a 8 de maio de 2024. Acedido a 20 de outubro de 2023. <https://www.ice.gov/mission>.
- Information Technology Bureau Los Angeles Police Department, e Dr. Craig D. Uchida. 2014. *Smart Policing: Institutionalizing Operation LASER in The Los Angeles Police Department*.

- Los Angeles: Justice & Security Strategies, Inc. <https://stoplapdspying.org/wp-content/uploads/2018/05/Program-Narrative.pdf>.
- Joint Regional Intelligence Center. s.d. "About the JRIC". Acedido a 4 de maio de 2023. <https://www.jric.org/default.aspx?MenuItemID=265&MenuSubID=111&MenuGroup=Public+Home>.
- Los Angeles Police Department. 2020. *Data-Informed Community-Focused Policing in the Los Angeles Police Department*. Los Angeles: Los Angeles Police Department. <https://lapdonlinestrgeacc.blob.core.usgovcloudapi.net/lapdonlinemedia/2021/12/data-informed-guidebook-042020.pdf>.
- Michelli, Thomas P. 2014. *Statement Regarding a Hearing On "Examining Challenges and Wasted Taxpayer Dollars in Modernizing Border Security IT Systems."* Before The U.S. House of Representatives Committee on Homeland Security Subcommittee On Oversight And Management Efficiency. U.S. Immigration and Customs Enforcement. <https://www.ice.gov/doclib/news/library/speeches/140206michelli.pdf>.
- MuleSoft. S.d. "O que é uma API? (interface de programação de aplicativos)." Acedido a 12 de novembro de 2023. <https://www.mulesoft.com/pt/resources/api/what-is-an-api>.
- Office of Mayor Mitch Landrieu. S.d. "NOLA, We Have A Problem." *NOLA For Life*. Acedido a 9 de outubro de 2023. <https://www.nolaforlife.org/home.html>.
- Office of the Director of National Intelligence. 2017. "How the IC works." ODNI. Acedido a 29 de julho de 2024. <https://www.intelligence.gov/how-the-ic-works/2-uncategorised>.
- Office of the Director of National Intelligence. S.d. "What is Intelligence?" ODNI. Acedido a 29 de julho de 2024. <https://www.dni.gov/index.php/what-we-do/what-is-intelligence>.
- Office of the Inspector General. 2019. *Review of Selected Los Angeles Police Department Data-Driven Policing Strategies*. Los Angeles Police Commission: Office of the Inspector General. http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf.
- Palantir Technologies. 2014. *NOLA Murder Reduction: Technology to Power Data-Driven Public Health Strategies White Paper*. DocumentCloud. Acedido a 18 de outubro de 2023. <https://s3.documentcloud.org/documents/4344816/NOLA-Murder-Reduction-White-Paper.pdf>.
- Palantir Technologies. 2015. "Philanthropy Engineering 2015 Annual Impact Report. Reducing Murder Rates." Acedido a 5 de agosto de 2023. Arquivado em <https://web.archive.org/web/20200218055502/https://www.palantir.com/philanthropy-engineering/annual-report/2015/murder-reduction/>.
- Palantir Technologies. 2020. "Palantir Apollo: Powering SaaS where no SaaS has gone before." *Medium*. Publicado a 29 de setembro de 2020. Acedido a 26 de abril de 2023. <https://blog.palantir.com/palantir-apollo-powering-saas-where-no-saas-has-gone-before-7be3e565c379>.
- Palantir Technologies. 2020b. *Form S-1 Registration Statement under The Securities Act of 1933*. United States Securities and Exchange Commission. Acedido a 12 de setembro de 2023. <https://www.sec.gov/Archives/edgar/data/1321655/000119312520230013/d904406ds1.htm>.

- Palantir Technologies. 2021. "Palantir Foundry 21 Launch | Demo Day." YouTube. Publicado a 3 de junho de 2021. Acedido a 19 de janeiro de 2023. <https://www.youtube.com/watch?v=h4R1cOIJ7o>.
- Palantir Technologies. 2022. "Homeland Security Investigations Renews Partnership with Palantir for Case Management Software that Support Investigations into Human Trafficking, Drug Smuggling, and Transnational Criminal Organizations." *Palantir Media*. Publicado a 26 de setembro de 2022. Acedido a 4 de junho de 2023. <https://www.palantir.com/newsroom/press-releases/homeland-security-investigations-renews-partnership-with-palantir/>.
- Palantir Technologies. s.d. "Gotham." *Palantir Technologies*. Acedido a 26 de julho de 2023. <https://www.palantir.com/platforms/gotham/>.
- Robertson, Duncan, et al. 2015. Crime Risk Forecasting. United States Patent 9,129,219 B1, registada a 30 de junho de 2014, e emitida a 8 de setembro de 2015. <https://patentimages.storage.googleapis.com/60/94/95/5dbde28fe6eea2/US9129219.pdf>.
- Sapphire. S.d. "Difference Between Information and Intelligence." Acedido a 29 de julho de 2024. <https://www.sapphire.net/blogs-press-releases/difference-between-information-and-intelligence/>.
- Schirmer, Sarah, e Jeff Asher. 2014. "HOBBITCON ° 3." Documento interno. DocumentCloud. Acedido a 18 de outubro de 2023. Arquivado em <https://www.documentcloud.org/documents/4344815-Nola-hc3-Final-20140403#document/p15>.
- Terry v. Ohio, 392 U.S. 1 (1968). <https://supreme.justia.com/cases/federal/us/392/1/>.
- The City of New Orleans Health Department. 2013. *The NOLA For Life PLAYbook: A Strategic Plan to Prevent Youth Violence in New Orleans*. https://nola.gov/getattachment/Health/Data-and-Publications/NOLA-FOR-LIFE-PLAYbook_for-web-9-2-14.pdf/.
- United States District Court Eastern District of Louisiana. 2013. "Amended and Restated Consent Decree Regarding the New Orleans Police Department." Acedido a 9 de outubro de 2023. <https://nola.gov/getattachment/NOPD/NOPD-Consent-Decree/Consent-Decree.pdf/>.

Fontes secundárias:

- Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation. Acedido a 21 de julho de 2023. <https://www.eff.org/cyberspace-independence>.
- Barrinha, André, e Thomas Renard. 2020. "Power and diplomacy in the post-liberal Cyberspace." *International Affairs* 96 (3): 750-767. <https://sci-hub.ru/10.1093/ia/iiz274>.
- Brayne, Sarah, e Angèle Christin. 2020. "Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts." *Social Problems* 68 (3): 608-624. <https://academic.oup.com/socpro/article-abstract/68/3/608/5782114?redirectedFrom=fulltext>.
- Brayne, Sarah. 2017. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82 (5): 977-1008. <https://doi.org/10.1177/0003122417725865>.

- Brayne, Sarah. 2020. "Dragnet Surveillance: Our Incriminating Lives." Em *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press EBooks. <https://doi.org/10.1093/oso/9780190684099.003.0003>.
- Brennan Center for Justice. 2017. "ICE Extreme Vetting Initiative: A Resource Page." Última atualização a 24 de maio de 2018. <https://www.brennancenter.org/our-work/research-reports/ice-extreme-vetting-initiative-resource-page>.
- Bullington, Jonathan, e Emily Lane. 2018. "New Orleans ends its relationship with tech firm Palantir, Landrieu's office says." *NOLA.com | The Times-Picayune*. Última atualização a 12 de julho de 2019. https://www.nola.com/news/crime_police/new-orleans-ends-its-relationship-with-tech-firm-palantir-landrieus-office-says/article_4a19a94e-3327-53af-971a-cd0d637f6dd9.html.
- Burgess, J. Peter. 2010. *The Routledge Handbook of New Security Studies*. Londres: Routledge.
- CATO Institute. 2023. "Surveillance Reform Prospects." CATO Surveillance Week 2023, 6 de junho. <https://www.cato.org/events/surveillance-reform-prospects>.
- Conor, Brian T., e Long Doan. 2021. "Government and corporate surveillance: moral discourse on privacy in the civil sphere." *Information, Communication & Society* 24 (1): 52-68. <https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2019.1629693>.
- Corsaro, Nicholas, et al. 2018. *Assessing the Long-Term Impact of Focused Deterrence in New Orleans: A Documentation of Changes in Homicides and Firearm Recoveries*. Office of Justice Programs' National Criminal Justice Reference Service. <https://www.ojp.gov/pdffiles1/nij/grants/254130.pdf>.
- Damin, Cláudio Júnior. 2013. "Segurança nacional e liberdades civis nos Estados Unidos: Obama e a opção pela segurança." *Boletim Meridiano* 47 14 (1399): 31-37. <https://periodicos.unb.br/index.php/MED/article/view/4775/4354>.
- Danaher, John. 2016. "The Threat of Algocracy: Reality, Resistance and Accommodation." *Philosophy & Technology* 29: 245-268. <https://link.springer.com/content/pdf/10.1007/s13347-015-0211-1.pdf>.
- Deibert, Ron. 2015. "The Geopolitics of Cyberspace After Snowden." *Current History* 114 (768): 9-15. <https://sci-hub.ru/10.1525/curh.2015.114.768.9>.
- Egbert, Simon. 2019. "Predictive Policing and the Platformization of Police Work." *Surveillance and Society* 17 (1/2): 83-88. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12920/8480>.
- Electronic Frontier Foundation. "Automated License Plate Readers (ALPRs)." EFF. Última atualização a 1 de outubro de 2023. Acedido a 21 de julho de 2023. <https://www.eff.org/pages/automated-license-plate-readers-alpr>.
- Electronic Privacy Information Center. S.d. "Patriot Act." EPIC. Acedido a 19 de junho de 2023. <https://epic.org/issues/surveillance-oversight/patriot-act/>.
- Feeney, Matthew. 2018. "Walling Off Liberty: How Strict Immigration Enforcement Threatens Privacy and Local Policing." *CATO Institute Policy Analysis* 852. <https://www.cato.org/policy-analysis/walling-liberty-how-strict-immigration-enforcement-threatens-privacy-local-policing>.

- Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press. <https://doi.org/10.18574/nyu/9781479854608.001.0001>.
- Fleury-Steiner, Benjamin. 2019. "Deportation Platforms: The AWS-ICE Alliance and the Fallacy of Explicit Agendas." *Surveillance & Society* 17 (1/2): 105-110. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12951/8482>.
- Foster, John Bellamy, e Robert W. McChesney. 2014. "Surveillance Capitalism. Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age." *Monthly Review* 66 (3). <https://monthlyreview.org/2014/07/01/surveillance-capitalism/>.
- Friedman, Barry, e Maria Ponomarenko. 2015. "Democratic Policing." Working paper No. 15-53. Vol. 90. *New York University School of Law*, novembro de 2015. <https://ssrn.com/abstract=2694564>.
- Goldberg, Jeffrey. 2015. "A Matter of Black Lives." *The Atlantic*, setembro de 2015. <https://www.theatlantic.com/magazine/archive/2015/09/a-matter-of-black-lives/399386/>.
- Hafermalz, Ella. 2021. "Book Review – The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power." *M@n@gement* 24 (4): 70-75. <https://management-aims.com/index.php/mgmt/article/view/5519/14165>.
- Harris, Mark. 2017. "How Peter Thiel's Secretive Data Company Pushed into Policing." *Wired*, 9 de agosto de 2017. <https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/>.
- Iliadis, Andrew, e Amelia Acker. 2022. "The Seer and the Seen: Surveying Palantir's Surveillance Platform." *The Information Society* 38 (5): 334-363. <https://doi.org/10.1080/01972243.2022.2100851>.
- Joseph, George. 2018. "The LAPD Has a New Surveillance Formula, Powered by Palantir." *The Appeal*, 8 de maio de 2018. <https://theappeal.org/the-lapd-has-a-new-surveillance-formula-powered-by-palantir-1e277a95762a/>.
- Knight, Emma, e Alex Gekker. 2020. "Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post- 9/11 Security Technology Infrastructures." *Surveillance & Society* 18 (2): 231-243. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13268/9303>.
- Landwehr, Marvin, Alan Borning, e Volker Wulf. 2021. "Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure." *Information, Communication & Society* 26 (1): 70-85. <https://doi.org/10.1080/1369118X.2021.2014548>.
- Levy, Jack S. 2008. "Case studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25 (1): 1-18. <https://www.jstor.org/stable/26275102?seq=1>.
- Liaropoulos, Andrew. 2016. "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics." *Journal of Information Warfare* 15 (4):14-26. <https://www.jstor.org/stable/pdf/26487548.pdf>.
- Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*. London:

- Routledge.
https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf.
- Lyon, David. 2007. "Surveillance, Security and Social Sorting: Emerging Research Priorities." *International Criminal Justice Review* 17 (3): 161-170.
<https://doi.org/10.1177/1057567707306643>.
- Marsh, David, Selen A. Ercan, e Paul Furlong. 2018. "A Skin Not a Sweater: Ontology and Epistemology in Political Science." Em *Theory and Methods in Political Science*, editado por Vivien Lowndes, David Marsh and Gerry Stoker. Bloomsbury Publishing PLC.
https://books.google.pt/books?hl=pt-PT&lr=&id=O5BKEAAAQBAJ&oi=fnd&pg=PP1&dq=David+Marsh,+Selen+A.+Ercan,+Paul+Furlong&ots=z0GpAwIDKE&sig=vAjRN3F2FI60QVgpP8O4Q40BfaM&redir_esc=y#v=onepage&q&f=false.
- Mijente. 2018. *Who's Behind ICE? The Tech and Data Companies Fueling Deportations*.
[https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE - The-Tech-and-Data-Companies-Fueling-Deportations- v1.pdf](https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE--The-Tech-and-Data-Companies-Fueling-Deportations-v1.pdf).
- Munn, Luke. s.d. "Seeing with Software. Palantir and the Regulation of Life." *Studies in Control Societies*. <https://studiesincontrolsocieties.org/seeing-with-software/>.
- Olesen, Thomas. 2022. "Whistleblowing in a time of digital (in)visibility: towards a sociology of 'grey areas.'" *Information, Communication & Society* 25 (2): 295-310.
<https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2020.1787484>.
- Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press. <https://archive.org/details/the-black-box-society-the-secret-algorithms-that-control-money-and-information-frank-pasquale/page/n3/mode/2up>.
- Pohle, Julia, e Leo Van Audenhove. 2017. "Post-Snowden Internet Policy: Between Public Outrage, Resistance and Policy Change." *Media and Communication* 5 (1): 1-6.
<https://www.cogitatiopress.com/mediaandcommunication/article/view/932/932>.
- Pohle, Julia, e Thorsten Thiel. 2020. "Digital sovereignty." *Internet Policy Review* 9 (4): 1-19.
<https://policyreview.info/pdf/policyreview-2020-4-1532.pdf>.
- Privacy International. 2020. "All roads lead to Palantir: A review of how the data analytics company has embedded itself throughout the UK." setembro de 2020. Acedido a 1 de dezembro de 2023. <https://privacyinternational.org/sites/default/files/2020-11/All%20roads%20lead%20to%20Palantir%20with%20Palantir%20response%20v3.pdf>.
- Puyvelde, Damien Van, Stephen Coulthart, e Mahmud Shahriar Hossain. 2017. "Beyond the buzzword: big data and national security decision-making." University of Glasgow, julho de 2017. <http://eprints.gla.ac.uk/144429/7/144429.pdf>.
- Richardson, Rashida, Jason M. Schultz, e Kate Crawford. 2019. "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice." *New York University Law Review* 94 (192): 192-233. <https://ssrn.com/abstract=3333423>.
- Sangiovanni, Andrea. 2019. "Democratic Control of Information in the Age of Surveillance

- Capitalism.” *Journal of Applied Philosophy* 36 (2): 212-216.
<https://onlinelibrary.wiley.com/doi/pdf/10.1111/japp.12363>.
- Schmidt, Eric, e Jared Cohen. 2013. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. Knopf Doubleday Publishing Group.
- Singer, Natasha. 2023. “Amazon to Pay \$25 Million to Settle Children’s Privacy Charges.” *The New York Times*, 31 de maio.
<https://www.nytimes.com/2023/05/31/technology/amazon-25-million-childrens-privacy.html>.
- Stanley, Jan. 2016. “Eight Problems With Police ‘Threat Scores.’” American Civil Liberties Union. Acedido a 18 de outubro de 2023. <https://www.aclu.org/news/privacy-technology/eight-problems-police-threat-scores?redirect=blog%2Ffree-future%2Feight-problems-police-threat-scores>.
- Stanley, Jan. 2018. “New Orleans Program Offers Lessons In Pitfalls Of Predictive Policing.” American Civil Liberties Union. Acedido a 18 de outubro de 2023. <https://www.aclu.org/news/privacy-technology/new-orleans-program-offers-lessons-pitfalls-predictive-policing>.
- Steinberger, Michael. 2020. “Does Palantir See Too Much?” *New York Times*, 21 de outubro de 2020. <https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html>.
- Stop LAPD Spying Coalition. 2021. *Automating Banishment. The Surveillance and Policing of Looted Land*. Los Angeles Community Action Network. Acedido a 17 de fevereiro de 2023. <https://automatingbanishment.org/assets/AUTOMATING-BANISHMENT.pdf>.
- Strange, Susan. 1995. “The Defective State.” *Daedalus* 124 (2): 55-74.
https://www.jstor.org/stable/pdf/20027297.pdf?refreqid=excelsior%3Aaa1dc9ad6ea4753b2ba99419a4c0133c&ab_segments=&origin=&initiator=&acceptTC.
- Strange, Susan. 1998. “What Theory? The Theory in Mad Money.” Working Paper No. 18/98. Centre for the Study of Globalisation and Regionalisation (CSGR), University of Warwick, dezembro de 1998. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=146958.
- Thomas, Ian. 2022. “Palantir CEO Alex Karp on the difference between fighting with Peter Thiel and progressives.” *CNBC*, 29 de junho. <https://www.cnbc.com/2022/06/29/palantir-ceo-karp-on-fighting-with-peter-thiel-and-progressives.html>.
- Tooze, Roger. 2010. “Susan Strange, Academic International Relations and the Study of International Political Economy.” *New Political Economy* 5 (2): 280-289.
<https://doi.org/10.1080/713687770>.
- Véliz, Carissa. 2022. *Privacidade é Poder. Por que razão e como devemos recuperar o controlo dos nossos dados*. Temas e Debates.
- Warren, Ian. 2015. “Surveillance, Criminal Law and Sovereignty.” *Surveillance & Society* 13 (2): 300-305.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law_sovereign/law_sov.
- Winston, Ali. 2018. “Palantir has secretly been using New Orleans to test its predictive policing technology.” *The Verge*, 27 de fevereiro.

<https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>.

Woodman, Spencer. 2016. "Transition Adviser Peter Thiel Could Directly Profit From Mass Deportations". *The Intercept*, 12 de dezembro. <https://theintercept.com/2016/12/12/transition-adviser-peter-thiel-would-directly-profit-from-mass-deportations/>.

Woodman, Spencer. 2017. "Palantir Provides The Engine For Donald Trump's Deportation Machine." *The Intercept*, 2 de março. <https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/>.

Zang, Dongsheng. 2022. "Revolt Against The U.S. Hegemony: Judicial Divergence in Cyberspace." *Wisconsin International Law Journal* 39 (1): 1-70. <https://repository.law.wisc.edu/s/uwlaw/media/303223>.

Zuboff, Shoshana. 2019. *A Era do Capitalismo da Vigilância. A Disputa por um Futuro Humano na Nova Fronteira do Poder*. Relógio D' Água.

Zuboff, Shoshana. 2019b. "'We Make Them Dance': Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights." Em *Human Rights in the Age of Platforms*, editado por Rikke Frank Jørgensen. The MIT Press.