



DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

MESTRADO EM RELAÇÕES INTERNACIONAIS

UNIVERSIDADE AUTÓNOMA DE LISBOA

“LUÍS DE CAMÕES”

**A PROBLEMÁTICA DAS CIDADES INTELIGENTES NO DIREITO À
PRIVACIDADE — OS CASOS DE LONDRES E DE AMESTERDÃO**

Dissertação para a obtenção do grau de Mestre em Relações Internacionais

Autora: Carolina Fragoso Marques

Orientador: General Luís Vasco Valença Pinto

Número da candidata: 30007188

Novembro de 2023

Lisboa

Agradecimentos

A realização desta dissertação foi exigente e valeu-me o apoio incansável daqueles que me rodeiam. Aos meus pais, o meu profundo agradecimento por sempre acreditarem em mim, por me apoiarem e por nunca me deixarem desistir. Estarei eternamente grata por tudo o que me ensinaram a ser.

Ao meu namorado, que sempre me incentivou a ser a melhor versão de mim mesma e me ajudou a ultrapassar tantos obstáculos.

À minha irmã, pelo companheirismo e pelo apoio.

Aos meus avós, que sempre me deram tanto carinho.

Ao meu orientador, que foi sempre incansável. Agradeço a paciência, a dedicação e o facto de se mostrar sempre disponível, mesmo nos momentos em que estava menos motivada. O alcance desta etapa da minha vida foi possível graças à sua persistência.

A todas as pessoas que, direta ou indiretamente, me deram força para continuar.

Resumo

O presente estudo tem como principal objetivo compreender o impacto que a evolução tecnológica tem nas Relações Internacionais e entender a interferência que o desenvolvimento tecnológico tem na privacidade da população. Paralelamente, e para que haja exemplos concretos em relação aos dados levantados, será feita uma análise entre as cidades de Londres e de Amesterdão. A escolha destas duas cidades recai sobre a importância que ambas têm para o espaço europeu, além de serem as cidades inteligentes mais desenvolvidas a nível da Europa, pelo que se torna interessante olhar para elas e compará-las com outras cidades inteligentes a nível mundial. Também será alvo de análise o nível de conhecimento que a população tem em relação à forma como os seus dados são tratados e, simultaneamente, da consciência de que os dados pessoais, ao serem inseridos no espaço virtual, se tornam bastante vulneráveis. Para fundamentar esta questão, foi realizado um questionário com o intuito de compreender a relação entre a frequência da utilização da *internet* e o conhecimento que as pessoas têm em relação aos perigos que enfrentam constantemente, mesmo que de forma inconsciente. É crucial analisar qual é o papel que as Relações Internacionais têm no impacto da evolução tecnológica e vice versa. Sendo o espaço virtual um espaço sem barreiras físicas, compreender o modo como se lida com as ameaças cibernéticas é extremamente relevante para compreender as Relações Internacionais atuais.

Palavras-chave: Cidade Inteligente; Proteção de Dados; Londres; Amesterdão

Abstract

The present research has the main goal of understanding the impact that technological evolution has on International Relations and understanding the interference of technologic development in people's privacy. At the same time, and in order to have concrete examples related with the collected information, it will be done an analysis between the cities of London and Amsterdam. The choice of these two cities falls under the importance that both have to the European espace, besides being the two most developed smart cities in Europe, therefore it is interesting to look at them both and compare them with other smart cities around the world. It will also be a target for analysis the level of knowledge that people have regarding the way their data is treated and, simultaneously, the consciousness that personal data, when inserted in the virtual world, becomes very vulnerable. To fundament this question, a questionnaire was made with the aim to understand the relation between the internet users and the knowledge people have about the dangers they face constantly, even if they're not conscious about it. It is crucial to analyse the role that International Relations have in the impact of technological evolution and vice versa. Being a virtual space a space without physical borders, understanding how can we deal with ciber threats is extremely relevant to also understand the current International Relations.

Keywords: Smart City; Data Protection; London; Amsterdam

Índice

Introdução	7
Capítulo 1 As Cidades Inteligentes	12
1.1. O conceito de Cidades Inteligentes	12
1.2. A progressão das Cidades Inteligentes.....	16
1.3. O impacto das Cidades Inteligentes para as Relações Internacionais	22
1.4. A aceleração 5G	25
Capítulo 2 O direito à privacidade e à segurança.....	28
2.1. A cibersegurança.....	31
2.2. A dificuldade na proteção de dados	39
Capítulo 3 Os casos de Londres e Amesterdão	50
3.1. O caso de Londres	50
3.2. O caso de Amesterdão	60
Capítulo 4 Resultados das Análises Comparativas	79
Conclusões	85
Referências Bibliográficas	88
Anexos	101
Anexo 1.....	102
Anexo 2.....	103
Anexo 3.....	110
Anexo 4.....	111
Anexo 5.....	112
Anexo 6.....	113

Anexo 7.....	114
Anexo 8.....	115

Índice de Figuras

Figura 1: Mapa da nova zona de Xiong'an e panorâmica do desenvolvimento.....	68
--	----

Introdução

Atualmente, é inevitável pensar numa sociedade dependente da tecnologia, mesmo nas mais pequenas ações diárias. A Inteligência Artificial (IA) e a Robótica são elementos cada vez mais vinculados tanto nas relações entre pessoas como entre países, pelo que o desenvolvimento de cidades inteligentes é uma realidade já palpável, principalmente nos países mais desenvolvidos onde a aposta em plataformas digitais se tem vindo a acentuar nos últimos anos. De facto, quando se mencionam cidades inteligentes referem-se cidades que priorizam a digitalização de serviços e que se servem da tecnologia para melhorar a qualidade de vida dos cidadãos. Depois, com o desenvolvimento da rede móvel 5G, o crescimento de cidades inteligentes tornou-se mais evidente, na medida em que passou a existir uma rede móvel com capacidade suficiente para acelerar esta conexão entre a cidade e a população através do mundo digital. Assim, existe uma alteração do panorama das relações interpessoais e interestatais que veio como consequência, direta ou indireta, da transformação das cidades e da sua opção pela entrega à tecnologia digital.

Por este motivo, esta investigação tem como principal objetivo analisar o desenvolvimento das cidades inteligentes e perceber o seu impacto no direito à privacidade. Inevitavelmente, durante esta análise serão analisadas quais as alterações que trazem para a forma como são estabelecidas ligações no âmbito das Relações Internacionais, não só nos seus benefícios, como também nas desvantagens que acarreta. É, por isso, essencial haver também uma análise do impacto que as cidades inteligentes têm nas relações entre países e perceber que riscos e dilemas podem trazer para a população. Por fim, no sentido de esclarecer o objetivo principal desta dissertação, é também vantajoso olhar para a capacidade de adaptação dos cidadãos face à evolução das cidades inteligentes e perceber que desafios enfrentam, bem como a postura que assumem relativamente a estes desafios.

Este tema tem bastante interesse na perspetiva das Relações Internacionais, uma vez que por trás dos inúmeros benefícios que a tecnologia trouxe para a vida dos cidadãos escondem-se também alguns riscos e desvantagens que facilmente passam, ou não, despercebidos, nomeadamente a nível da segurança humana. Embora o conceito se mantenha, as ameaças transnacionais não têm o mesmo impacto que tinham no século passado, considerando que o *modus operandi* sofreu alterações, não só pelo recurso ao ciberespaço, como também no poder que a informação tem e no modo como se manipula sons e imagens.

Atualmente, as ameaças à segurança humana ultrapassaram o espaço físico e a exposição dos civis às ameaças transnacionais aumentou a olhos vistos. Luís Elias (2016), quando se refere à criminalidade atual menciona: “Trata-se de uma criminalidade com uma dimensão supranacional, não se limitando às fronteiras da soberania dos Estados-Nação, fluida, flutuante, múltipla, volátil e mimética, onde as conexões entre crime organizado e crime de rua são cada vez mais uma constante”¹. Neste sentido, são dissolvidas as fronteiras geográficas, o que poderá pôr em causa a Segurança Internacional, uma vez que as ameaças garantem um cariz global onde esta nova criminalidade tem como base o recurso à tecnologia e ao ciberespaço para atingir tanto pessoas como Estados. Este é um aspeto relevante para as Relações Internacionais, já que a mudança de paradigma das ameaças transnacionais compromete a segurança da população e afeta as infra-estruturas estatais criadas no sentido de manter a paz e promover a segurança, tornando-as desatualizadas. As novas formas de ataque contornam aquilo que são os métodos de defesa em curso e é inevitável que as infraestruturas de segurança acompanhem este novo ritmo, pois só assim conseguirão garantir a sua eficiência.

É também certo que a vulnerabilidade dos dados pessoais é cada vez mais uma realidade que se encontra à distância de um ataque informático. São tantos, e há todos os dias milhares de tentativas de ataque, que se torna difícil fazer um inventário de todos eles. É por isso de realçar a importância que o investimento na cibersegurança tem e a prioridade que deveria ser dada a este investimento não só em qualquer empresa, mas também na sociedade e no próprio Estado. De todas estas dimensões, não restam dúvidas de que o investimento na cibersegurança no Estado tem uma relevância muito maior, uma vez que é detentor de informações de cariz pessoal importantes e que muitas vezes não estão devidamente protegidas.

Existem cada vez mais exemplos desta vulnerabilidade que pode ser utilizada tanto para interesses políticos, através da ciberspionagem, como por exemplo também no setor da saúde, através da venda de dados pessoais em domínios como a *darkweb*. Este tipo de episódios violam o direito fundamental de proteção de dados pessoais, consagrado no Artigo 8.º d’ A Carta dos Direitos Fundamentais da União Europeia — “1. Todas as pessoas têm

¹ ELIAS, Luís — Criminalidade Transnacional Organizada. Paradoxos Conceptuais e Desafios Políticos e Operacionais. In BORGES, João Vieira [et al.] — **Ameaças e Riscos Transnacionais no Novo Mundo Global**, p. 119.

direito à protecção dos dados de carácter pessoal que lhes digam respeito”² — e são cada vez mais recorrentes, tendo em conta a exposição a que os dados pessoais estão sujeitos.

Assim, num mundo em que a tecnologia está intrínseca na grande maioria das atividades diárias, é importante que a legislação acompanhe este avanço, já que pode pôr em causa um direito fundamental. Por isso, pretende-se fazer uma análise do dilema do direito à privacidade numa sociedade onde cada vez mais é necessário prescindir desse direito para que se possa usufruir da segurança e das vantagens trazidas pela IA e pela Robótica. Sabemos hoje que uma das capacidades mais atrativas da IA é a análise massiva de dados num curto espaço de tempo — hoje já existem *chats* de Inteligência Artificial, como o *ChatGPT*, com a capacidade para, em questão de segundos, fazer análises detalhadas sobre qualquer assunto. O algoritmo da IA tem bastante peso nas relações internacionais pelo peso que tem a informação a que é capaz de aceder: desde descobertas científicas, até ao armamento militar. Aliás, no âmbito da Defesa, tanto a IA como a Robótica potencializam a defesa e segurança internacionais através do desenvolvimento de capacidades das infra-estruturas para detetarem comportamentos anómalos, o que agiliza o combate a ataques cibernéticos. A par desta capacidade, é também possível a análise de um avolumado número de dados passíveis de serem usados na prevenção de futuros ataques e de reconhecer os padrões destes mesmos ataques. É, por isso, inevitável usar este recurso fundamental como forma de prevenir possíveis ofensivas e é possível consegui-lo não só através do melhoramento de drones na vigilância e patrulhamento de fronteiras, por exemplo, como também através da configuração de novas armas e veículos de defesa.

Tendo em conta todos estes fatores, e no seguimento daquilo que foi definido como objetivo principal, é também importante para esta investigação analisar o desenvolvimento das cidades de Londres e Amesterdão no domínio tecnológico e que impactos estará a ter este factor na vida dos cidadãos que nelas habitam. Este tema constituirá o objetivo secundário desta dissertação.

Neste sentido, esta dissertação, no seu primeiro capítulo, começa pela explicação dos conceitos importantes para a compreensão deste tema como, por exemplo, a explicação do conceito de cidades inteligentes e o modo como estão a progredir. Também é importante trazer para este capítulo uma contextualização do impacto que, por via disso, estas cidades

² Jornal Oficial da União Europeia — **A Carta dos Direitos Fundamentais da União Europeia: Artigo 8.º** [Em linha].

têm nas Relações Internacionais, bem como a aceleração que estão a sofrer com a chegada da rede móvel 5G.

Num segundo capítulo, é abordado o direito à privacidade e à segurança, com foco, principalmente, na cibersegurança e na dificuldade que existe na proteção de dados. É aqui importante perceber se o direito à privacidade pode, ou não, ser afetado pelas cidades inteligentes, além de analisar o modo como este fator e as próprias cidades inteligentes afetam ou influenciam as relações internacionais. Por isso, neste capítulo serão ainda analisados os resultados de um questionário elaborado com o intuito de compreender se a população está consciente dos riscos que enfrentam enquanto utilizadores da *internet* e do conhecimento que têm em relação a este tema.

Já o terceiro capítulo é direcionado para uma análise do estado atual das cidades de Londres e de Amesterdão enquanto cidades inteligentes, para assim se perceber de que forma estão a progredir, que estratégias estão a adotar e de que modo enfrentam os desafios atuais. É adequado que este estudo se foque em cidades europeias, não só pela facilidade de acesso à informação, mas também pela importância e valor que estas cidades trazem para o espaço europeu. É ainda fundamental perceber quais os riscos reais que as cidades inteligentes enfrentam no direito à privacidade e qual o papel que a Comissão Europeia tem na tentativa de dissuadir estes riscos, um fator inerente do decurso da análise do objetivo secundário traçado.

De facto, é fundamental averiguar casos reais, uma vez que através deste estudo será possível esclarecer o estado atual das cidades inteligentes visando, principalmente, compreender o significado da sua posição e do seu impacto a nível internacional. Neste sentido, Londres e Amesterdão, sendo duas cidades europeias influentes, permitem-nos considerar a sua posição no quadro internacional, mesmo quando comparadas com cidades inteligentes fora do espaço europeu.

Por fim, no quarto capítulo será feita uma análise comparativa entre Londres e Amesterdão com uma exposição dos resultados deste estudo, bem como as conclusões e os principais aspetos a retirar desta análise. Evidentemente, todo este cenário tem um grande impacto nas Relações Internacionais, como irá ser analisado ao longo desta dissertação.

Metodologia

Esta investigação seguiu, primeiramente, uma metodologia qualitativa através da revisão de literatura, incluindo o estado da arte e formulação de questões e associações relativas à forma como a tecnologia está a influenciar as Relações Internacionais. Além disso, seguiu-se também uma metodologia quantitativa, embora menos abrangente, com a realização de um questionário que teve como principal objetivo entender a percepção das pessoas relativamente ao fornecimento e tratamento dos seus dados pessoais na *internet*. Para esse fim, foram inquiridas 105 pessoas de diversas faixas etárias, sendo a faixa etária entre os 18 e 24 anos a mais abrangente e com mais aderência.

Por último, esta investigação teve ainda como base de análise episódios recentes noticiados em diversos órgãos de comunicação social públicos, além de revisão da legislação em vigor, principalmente, no Espaço Europeu, tendo sempre em vista o impacto e a importância do tema para as Relações Internacionais.

Capítulo 1 | As Cidades Inteligentes

Neste capítulo será abordado o que são as cidades inteligentes e será colocada em evidência a importância que estas têm não só no direito à privacidade, como também nas relações internacionais. Efetivamente, a alteração da dinâmica das cidades influencia diretamente o modo como se relacionam entre si e, conseqüentemente, a sua posição perante as relações que têm com outros países. A título de exemplo, o aumento da circulação de informação no ciberespaço altera as vulnerabilidades das cidades e o seu *modus operandi* perante a Comunidade Internacional. Por um lado, porque a informação ganhou mais importância, tornando-se mais valiosa, a partir do momento em que através do seu acesso se pode pôr em causa a segurança da própria cidade, o que a torna mais vulnerável. Por outro lado, porque existe um número massivo deste tipo de informação onde, a partir do momento em que todos os detalhes sobre a cidade e sobre os cidadãos circulam no ciberespaço, ficam à distância de um ataque informático. Desta forma, é inevitável que as relações e as preocupações de cidades inteligentes sejam diferentes daquilo que eram as relações e preocupações das cidades que carecem de tecnologia e que não dominam o ciberespaço.

Além disso, atualmente as cidades com maior desenvolvimento tecnológico são as cidades que detêm maior poder económico, sendo, deste modo, o avanço tecnológico um fator importante para a definição da hierarquia das potências mundiais.

A verdade é que a tecnologia e a evolução das relações humanas através do ciberespaço poderão contribuir em grande escala para a alteração dos cenários que hoje são para nós uma realidade, mas também tornam evidente a tendência que existe e que poderá culminar na prevalência de cidades inteligentes sobre cidades menos desenvolvidas tecnologicamente.

1.1. O conceito de Cidades Inteligentes

Atualmente, uma cidade inteligente define-se como uma cidade onde a tecnologia lidera o dia a dia das pessoas e onde tudo está virtualmente conectado. Descreve, por isso, o modo como a tecnologia responde às necessidades da população de forma a melhorar a sua qualidade de vida. No fundo, uma cidade inteligente é mais eficiente, mais sustentável e mais conectada e, por isso, mais apelativa.

De facto, a evolução tecnológica, principalmente com a chegada da tecnologia 5G, tem trazido uma aceleração da tecnologia e uma nova forma de percepção sobre o modo como nos envolvemos perante as cidades inteligentes. O 5G vem trazer uma alteração ao modo de vida e uma aceleração destas cidades, na medida em que existem mais cidades inteligentes e que se desenvolvem mais depressa face à evolução tecnológica e à progressiva digitalização da própria cidade, espelhada numa população que adere e aceita este progresso. Tendo em conta que a principal característica da rede móvel 5G é a melhoria da velocidade da *internet*, a chegada do 5G traz consigo um aumento na conexão da *Internet* das Coisas (*IoT*)³, essencial para o desenvolvimento das cidades inteligentes. Evidentemente, esta aceleração torna inelutável o impulsiono do crescimento económico de uma cidade e impulsiona a construção de ambientes mais inclusivos. Neste contexto, o aumento do número de cidades inteligentes tende a aumentar progressivamente, o que, inevitavelmente, culminará na modificação das Relações Internacionais vigentes que passaram a reger-se cada vez mais por uma relação cibernética e que envolve informação sensível sobre a própria população, uma causa/consequência do envolvimento da *IoT* no quotidiano das pessoas. Além disso, se existe um maior envolvimento tecnológico na economia da cidade, é natural que este seja um fator constante nas relações entre pessoas, cidades e Estados. Por isso, quanto mais cidades inteligentes houver e quanto mais desenvolvidas forem, maior será o envolvimento que, inevitavelmente, se fará sentir nas suas próprias relações, inclusive no âmbito internacional, o que não se verificava no final do século XIX e início do século XXI por não haver uma aproximação tão afincada entre pessoas, cidades e nações.

De modo a incrementar este universo de ligação entre coisas e pessoas, surgem as redes *LoRaWAN*⁴, um tipo de tecnologia que impulsionou a *IoT*, já que a implantação destas duas redes, a 5G e a *LoRaWAN*, se caracteriza por ser um tipo de protocolo de comunicação sem fios que permite que os dispositivos da *IoT* enviem e recebam dados de plataformas de gestão. Ou seja, para que haja comunicação entre dispositivos inteligentes é necessária uma comunicação entre estes dispositivos e plataformas de gestão e a rede *LoRaWAN* permite estabelecer esta ligação numa área muito mais vasta, mas ao mesmo tempo usando baixa

³ *Internet of Things*, na sigla inglesa.

⁴ *Long Range Wide Area Network*, na sigla inglesa.

potência⁵. A implementação destas duas redes é inerente ao uso da *IoT*, uma vez que permite que a sua utilização pelas pessoas se torne muito mais económica e sobretudo mais rápida e mais eficaz. Comparativamente com a rede 5G, a rede *LoRaWAN* tem um alcance maior e menor consumo, sem descartar a utilidade que a rede 5G traz para a aceleração da *IoT* através da capacidade de estabelecer comunicações rápidas.

Tendo em conta este cenário, é importante notar que fazer a instalação destes sistemas numa cidade exige poder económico, o que leva a que haja um desequilíbrio evidente entre os países desenvolvidos e os países em desenvolvimento. Por outro lado, o surgimento da ciberespionagem, do cibercrime e, até, da própria cibersegurança, condiciona aquilo que são as tradicionais Relações Internacionais, tornando-se crucial a introdução da tecnologia e do uso da IA a seu favor.

Ainda relativamente à *IoT*, esta a mais não corresponde do que a dispositivos conectados entre si, isto é, define-se pelo uso da *internet* em pequenos gestos, utensílios e equipamentos como, por exemplo, frigoríficos inteligentes, carros inteligentes, robôs de cozinha inteligentes, entre tantos mais. A conexão da *IoT* é assim promovida pela aceleração da rede 5G o que, consequentemente, ajuda a promover as cidades inteligentes, caracterizadas pela conexão das pessoas aos dispositivos e pelo uso da *internet* nas atividades e ações diárias — “IoT connects people with physical objects, such as vehicles, home appliances, and smartphones enabling them to communicate with each other, sharing data to produce intelligent services and improve quality of life”⁶.

Embora as vantagens sejam diversas, surgem também cada vez mais algumas desvantagens associadas à nossa exposição ao ciberespaço, como irá ser exposto adiante. Na verdade, o grande objetivo das cidades inteligentes é dotarem-se com a tecnologia necessária para serem capazes de servir os seus habitantes e promover a melhoria da sua qualidade de vida — “Improving the quality of life of citizens is a central concept, and we assume it to be an ultimate goal of SC [Smart Cities] developments”⁷.

⁵ Sem autor — **What is LoRaWAN?** [Em linha]. In Caburn Telecom, sd.

⁶ CRANMER, Elenor E. [et al.] — Internet of Things: Aspiration, implementation and contribution. **Journal of Business Research** [Em linha]. vol. 139 (2022), p. 69.

⁷ CSUKÁ, Máté S.; SZABÓ, Roland Z. — The many faces of the smart city: Differing value propositions in the activity portfolios of nine cities. **Cities** [Em linha]. vol. 112 (2021) p. 3.

Deste modo, o recurso à Inteligência Artificial é o denominador comum destas cidades e é fulcral para que uma cidade possa ser considerada inteligente. A automação e a robotização também fazem parte deste leque de serviços que, uma vez sendo parte do ciberespaço, são capazes de fornecer respostas mais rápidas e com melhor qualidade à população. Essencialmente, a conexão de um serviço à *internet* permite que a circulação de dados no mundo virtual facilite o dia a dia de todos os habitantes dessas cidades, tendo em conta que torna todas as respostas mais instantâneas e que vai ao encontro das necessidades individuais. Em suma, estamos perante um serviço mais personalizado, mais rápido e mais eficaz.

Hoje podemos ainda referir o *ChatGPT*, um *chat* com Inteligência Artificial e com a capacidade para, apenas em segundos, responder minuciosamente e com bastante precisão a qualquer tipo de questão. Com o detalhe algorítmico que esta ferramenta tem é possível elaborar um artigo minucioso e correlacionar diversos campos das mais diversas áreas. Já foram feitos vários testes por muitos especialistas em diferentes áreas e todos salientaram o facto de esta ferramenta ter vindo revolucionar a perspectiva da evolução a curto prazo⁸.

A versão mais recente desta ferramenta, o *ChatGPT plus*, fornece ao utilizador uma resposta com base em informação *up-to-date*⁹, ou seja, é possível fazer uma análise atualizada e com base em informação fornecida pelo ciberespaço atual. No entanto, como este *chat* não conhece o que é certo ou errado, pode até basear-se em informação falsa que assume como sendo correta. Este tipo de riscos recomenda que a análise da resposta careça de uma opinião humana para corroborar os factos, tornando as suas respostas mais credíveis.

Não obstante, Laura Puttkamer, uma jornalista urbana, conversou com o *ChatGPT*¹⁰ com o objetivo de testar as respostas dadas pela IA relativamente às *Smart Cities* e divulgou importantes e coerentes resultados com bastante impacto para os projetos previamente analisados. Salvaguardando que este tipo de interação foi feito com a primeira ferramenta de IA (pelo menos revelada a público), a verdade é que a análise das respostas dadas pelo *chat* se revelam muito superficiais. A título de exemplo, quando Puttkamer pergunta ao *ChatGPT* quais são os perigos da IA no planeamento urbano, o *ChatGPT* limita-se a referir

⁸ GOODE, Lauren — **Review: We Put ChatGPT, Bing Chat, and Bard to the Test** [Em linha]. In Wired, 2023.

⁹ Natalie — **ChatGPT — Release Notes** [Em linha]. In OpenAI, 2023.

¹⁰ PUTTKAMER, Laura — **Interview with Chat GPT on the Smart City** [Em linha]. In Bee Smart City, 2023.

superficialmente aspetos como a automação, a proteção de dados, a falta de transparência, entre outros, sem nunca abordar estes parâmetros de forma clara e fundamentada, limitando-se a listar um grupo de desafios¹¹.

Por outro lado, um dos maiores benefícios desta ferramenta tem sido a sua ajuda na automatização de programas em diversas áreas. Desde pedir para criar um vídeo com voz, textos e imagens sobre qualquer tema, até à elaboração de código para ajudar engenheiros de sistemas e programação a criar ou completar tarefas complexas. A verdade é que a Inteligência Artificial tem permitido explorar um leque muito vasto de perspetivas, não só para a evolução da tecnologia atual como para a criação de novos projetos.

Neste sentido, devemos olhar para as cidades inteligentes como cidades que tiram proveito do mundo virtual e do ciberespaço para crescer e oferecer serviços com melhor qualidade aos seus habitantes, sempre apoiadas e alavancadas pelos avanços mais recentes da Inteligência Artificial.

1.2. A progressão das Cidades Inteligentes

O termo *cidade inteligente* começa por surgir em 1970 quando em Los Angeles se criou o primeiro projeto de dados urbanos, muito embora a primeira cidade realmente inteligente remonte a 1994 quando Amesterdão criou a sua primeira cidade virtual, *De Digital Stad*. Este projeto simulou uma cidade virtual e apelava a que os seus utilizadores utilizassem aquela ideia de cidade para a comunidade real. Por outras palavras, a primeira versão do projeto *De Digital Stad* não foi mais do que uma experiência e simulação de um espaço virtual, onde os seus utilizadores podiam andar pelas ruas de uma cidade virtual, permitindo, numa fase mais avançada, que cidadãos pudessem, por essa via, utilizar os mesmos serviços correntemente disponibilizados por uma cidade, tais como cafés, correios, etc.¹².

Se em 1994 Amesterdão já retinha esta perceção de uma cidade virtual, onde havia serviços públicos interligados pela *internet*, um estudo feito pelo *Global Data* estima que em 2050 cerca de 70% da população mundial viva já numa cidade inteligente¹³. Estes números

¹¹ Idem.

¹² ALBERTS, Gerard [*et al.*] — Archaeology of the Amsterdam digital city; why digital data are dynamic and should be treated accordingly. **Internet Histories** [Em linha]. 1:1-2 (2017), p. 149.

¹³ GlobalData Thematic Research — **History of smart cities: Timeline** [Em linha]. In Verdict, 2020.

deixam-nos motivo para reflexão sobre o impacto internacional que terá o aumento do número de cidades inteligentes na geopolítica e nas relações entre Estados, isto porque a política e o desenvolvimento económico¹⁴ não podem deixar de ser afetados pela mudança de paradigma, seja esta mudança feita mais rápida ou mais lentamente.

Segundo Li Bing (2022), uma cidade inteligente é controlada por seis fatores: sociedade inteligente, orçamento inteligente, paisagem inteligente, habitação inteligente, plataforma e sociedade inteligente¹⁵, pelo que é inevitável haver uma relação entre desenvolvimento tecnológico e crescimento económico. No entanto, é certo que também é preciso haver poder económico para haver um desenvolvimento tecnológico, pelo que um dos principais fatores a apontar será o aumento de desigualdade entre países, uma vez que os países desenvolvidos terão mais poder económico para fazer crescer tecnologicamente as suas cidades e os países em desenvolvimento não conseguirão acompanhar essa aposta em tecnologia. À medida que se vai investindo em tecnologia mais rápida existe um consequente crescimento da cidade em questão, pelo que o fosso entre estes países será cada vez mais palpável. Esta relação irá pôr em causa não só a população mais pobre, mas também a classe média que não vai conseguir acompanhar o crescimento da população mais rica, criando-se assim uma disparidade muito maior. Neste contexto, Carlos Moedas, atual Presidente da Câmara de Lisboa, faz uma observação bastante relevante numa entrevista com Pedro Pinto, na qual evidenciou esta disparidade não só entre a sociedade, mas também entre países — “Trata-se de uma desigualdade que não é só entre ricos e pobres. É também entre os ricos, que ficaram muito mais ricos, e a classe média, que ficou mais pobre. E ainda uma desigualdade entre as cidades e a província, entre as metrópoles e o interior. Aquilo que terá de ser feito nos próximos anos é pensar em como civilizar a globalização. [...] na área fiscal encontramos uma desigualdade enorme no mundo, em que as empresas digitais, por serem mundiais e globais, praticamente não pagam impostos. [...] Têm de ser os governos com medidas a conseguir fazer esta mudança”¹⁶.

¹⁴ Ver anexo 1.

¹⁵ BING, Li — Effective energy utilization through economic development for sustainable management in smart cities. **Energy Reports** [Em linha]. vol.8 (2022), p. 4978.

¹⁶ PINTO, Pedro — **Conversas Globais: as grandes questões geopolíticas, nacionais e internacionais**, pp. 33-34.

A realidade é que um Estado com poderosas cidades inteligentes será um Estado com mais poder económico e, consequentemente, com maior capacidade para investir em empresas e apoiá-las. Pegar nestas empresas e deslocá-las para países onde a mão de obra é mais barata, vai resultar na diminuição dos custos de produção, por um lado, e num lucro muito maior para a empresa, tendo em conta as ajudas do estado, por outro lado. Perante este cenário, as empresas locais não terão hipótese de concorrência, o que culmina num ciclo vicioso e na disparidade referida acima, já que as empresas estrangeiras irão lucrar, crescer e enriquecer e as empresas locais não terão a capacidade de acompanhar esta concorrência, acabando por falir e trazer desemprego, prejuízo e estagnação para o país, em prol do enriquecimento de outro país. A título de exemplo, o crescimento económico da China tem sido evidente e o seu investimento na tecnologia e no digital impulsionou esta tendência. Desde 2013 que a China tem um plano económico para penetrar em países europeus, africanos e asiáticos e aí sediar empresas chinesas, abrindo assim as suas portas ao mundo. Este plano económico ficou conhecido como *Nova Rota da Seda*¹⁷ e, segundo Abel de Freitas, jornalista d'O jornal Económico, “Para Pequim, a Nova Rota da Seda é a grande estratégia económica e de cooperação internacional que irá construir uma nova ordem económica mundial que substituirá a instituída pós-Segunda Guerra Mundial, sob a tutela dos EUA”¹⁸. Esta estratégia político-económica chinesa ambiciona atuar em vários setores e esta possibilidade advém do poder tecnológico chinês — os investimentos são para serem feitos não só em setores como o portuário, a energia, a telecomunicação, mas também no digital e na saúde¹⁹. Efetivamente, a China sempre assumiu uma posição estratégica que nunca foi de ofensiva militar. Faz parte do seu ADN e da sua cultura conquistar pela estratégia e nunca pela força, pelo que o seu envolvimento em conflitos externos não existe, ao passo que continuam a auferir vantagens através de estratégias políticas que resultam a seu favor. A *Nova Rota da Seda* mais não é do que uma política económica externa que pretende expandir o comércio chinês e, consequentemente, alargar a sua área de influência sem nunca demonstrar supremacia através da força. Neste sentido, vê-se uma China empenhada na expansão do seu domínio externo e não é por acaso que também a China lidera a tecnologia de ponta e está focada em

¹⁷ *One Belt, One Road*, na sigla inglesa.

¹⁸ FREITAS, João Abel de — **A Nova Rota da Seda** [Em linha]. Lisboa: O Jornal Económico, 2021.

¹⁹ Idem.

desenvolver as suas cidades de tecnologia inteligente enquanto incentiva também a criação de novas cidades inteligentes de raiz e dotadas de serviços apoiados na Inteligência Artificial.

Apesar deste grande impulso chinês, vemos que a aceleração tecnológica tem vindo a acentuar-se e alterar a geopolítica em todo o lado, refletida também no crescimento e desenvolvimento das cidades inteligentes por todo o mundo. Desde as transações financeiras até à comunicação pessoal entre cidadãos, a transformação e a conexão ao ciberespaço é inevitável e, por isso, existe uma clara redefinição de cidades por todo o mundo. Este é um cenário que se foi tornando evidente à medida que a população começou a mudar de comportamentos, consequência da adesão à tecnologia. Um exemplo muito simples, mas que retrata muito bem este argumento, são as empresas de transporte de mercadoria e de correio. No século passado, os serviços de correio tinham muita adesão, pois toda a informação circulava por cartas: desde correspondências pessoais, a fiscais. Com a chegada dos SMS e do correio eletrónico esta realidade mudou completamente. Atualmente, qualquer comunicação feita aos cidadãos vem por email, as faturas em certas lojas e supermercados também já nos chegam por email, e a comunicação pessoal definitivamente já só funciona com recurso à *internet*. Ora, neste contexto, poderia ser fácil concluir que a necessidade destas empresas de transporte de mercadorias e dos correios se extinguisse, mas a verdade é que, também consequência do uso da *internet*, as encomendas *online* dispararam e hoje em dia são indispensáveis para o conforto da população. Com isto, as transações monetárias são muito recorrentes e recorre-se à *internet* para fazer qualquer tipo de pagamento: seja de uma compra *online*, seja de uma transferência pessoal. No espaço de menos de cinquenta anos, o modo de vida alterou-se significativamente, consequência do uso da *internet*. Todo este recurso à *internet* requer que a informação circule no ciberespaço e quanto mais inteligente é uma cidade, melhores serviços e recursos consegue entregar à sua população.

Desde 2020 que houve um crescimento no recurso à tecnologia, uma vez que o cenário pandémico a isso obrigou numa escala mundial. Neste sentido, embora tenha havido um progresso tecnológico até 2020, este foi um ano crucial para a sua implementação pela necessidade que houve na utilização de serviços remotos. Existem vários exemplos deste progresso, seja no debate político internacional, no ensino à distância, no teletrabalho, na telemedicina ou mesmo nas compras *online*. Tudo o que era possível converter de presencial para remoto sofreu um crescimento exponencial, o que contribuiu bastante para a

consciencialização do inevitável desenvolvimento das cidades inteligentes que se viram obrigadas a crescer na esteira da nova realidade. De todas as áreas, a área da saúde foi uma das que teve um desenvolvimento tecnológico mais notável nos últimos cinco anos, nomeadamente na abordagem ao paciente com a adoção da telemedicina, onde o paciente pode ser consultado no conforto do seu lar através de uma videochamada. As vantagens são inúmeras, desde a diminuição de filas de espera em hospitais e centros de saúde até à rapidez com que o profissional de saúde pode chegar a quem procura ajuda médica. Segundo Miguel Aguiar, Diretor do Cluster Novos Cuidados da CUF, a telessaúde procura a proximidade, mas também a prevenção e atualmente já é possível fazer teleconsultas além fronteiras, havendo sempre a garantia de prestação de cuidados de saúde mesmo estando fora do país²⁰. Além disso, outro grande passo dado a favor dos utentes e que recorreu à tecnologia de ponta foi, sem dúvida, a hospitalização domiciliária, onde é feita remotamente a monitorização dos pacientes que precisam de estar a ser vigiados continuamente, principalmente nos cuidados paliativos. Estas opções acarretam largas vantagens, não só relativas ao conforto do próprio paciente, mas também na libertação de camas nos hospitais e na maior abrangência de resposta para com os utentes. Para que estas ofertas sejam possíveis, é necessário que haja não só hospitais e centros de saúde com tecnologia suficiente para a entrega do serviço, como também a formação de profissionais de saúde capazes de lidar com esta nova forma de chegar aos utentes.

Por outro lado, a automatização das indústrias é um dos fatores mais importantes no âmbito das cidades inteligentes, uma vez que é um dos setores que mais contribui em grande escala para a concretização da ligação de uma cidade ao ciberespaço. De facto, fala-se cada vez mais de uma Indústria 5G, ou seja, uma indústria que visa produzir com mais eficiência, tendo por base o avanço tecnológico, contribuindo para um crescimento económico mais estável, com uma rentabilidade cada vez mais alta e com a finalidade de servir as pessoas com mais qualidade — “Industry 5.0 provides a vision of industry that aims beyond efficiency and productivity as the sole goals, and reinforces the role and the contribution of industry to society”²¹.

²⁰ AGUIAR, Miguel — **O Digital ao Serviço da Saúde: da Telemedicina à Medicina ao Domicílio: Necessidades e Oportunidades a Nível Local**. Lisboa: Smart Cities Summit Portugal, 12 de outubro de 2023.

²¹ European Commission, Directorate-General for Research and Innovation — **Industry 5.0: human-centric, sustainable and resilient** [Em linha]. In Publications Office, 2021.

Neste sentido, o progresso das cidades inteligentes já é um processo em curso e está cada vez mais associado ao bem-estar da sociedade, pelo que a tecnologia é usada em benefício das pessoas e não com o objetivo de as substituir — “A feature of Smart Cities in the West is that development is mainly bottom-up, with the private sector and citizens actively engaging in designing projects to improve the quality of life, drive economic growth, and safeguard the environment”²².

Ora, seguindo esta ordem de ideias, que impacto tem este crescimento avultado destas cidades para a ordem mundial? É certo que durante toda a História pudemos ver crescimento e progressão. Desde os primeiros povos até aos dias correntes, a verdade é que não houve um momento em que não houvesse inovação, descobertas e novos recursos. No entanto, e segundo Kissinger (2017), o que marca tanto a nossa época é a velocidade com que as novas descobertas surgem e o poder que esta propagação tecnológica de informação tomou e que culmina numa fusão entre o espaço físico/urbano e o ciberespaço²³. Efetivamente, no período do pós-Guerra Fria, o mundo ambicionava a paz, animados por um momento de cessação de conflito, pelo que foi inquestionável a imposição sobre a inviolabilidade de fronteiras. Nesta ordem mundial, liderada pelos EUA, o poder unilateral fazia-se sentir, sobre a influência de um Estado democrático e entusiasmado por estabelecer relações diplomáticas de conversa e negociação com outros países, o que garantia a paz mundial. No entanto, o desenvolvimento tecnológico levou a um desabar destas fronteiras e aquilo que há cerca trinta anos se tornou uma realidade inquestionável é agora posto à prova. A *internet* eliminou as barreiras físicas da informação e qualquer chefe de Estado se vê obrigado a comentar qualquer acontecimento (seja ele social, político ou económico) fora das suas fronteiras, sob pena do julgamento social, sendo por isso bastante comum a utilização dos meios de comunicação social para mostrar a posição dos chefes de Estado no que diz respeito a diversos assuntos com um peso relevante para a ordem mundial. Todos os chefes de Estado declararam o seu parecer relativamente à atual Guerra na Ucrânia, ou à situação no Médio Oriente, bem como a assuntos de cariz social e político, como atentados e catástrofes naturais.

²² CARRIER, Frédérique — **How are Smart Cities meeting the challenges of urbanization in the 21st century?** [Em linha]. In RBC Wealth Management, sd.

²³ KISSINGER, Henry — **A Ordem Mundial: Reflexões sobre o carácter das Nações e o Curso da História**, p. 392.

Além disso, e a título de exemplo, a Primavera Árabe mostrou ser um dos pontos de viragem sobre a intervenção das redes sociais em matéria política e social. Graças a elas, manifestações na Tunísia passaram fronteiras e geraram protestos em todo o Norte de África e Médio Oriente e, por isso, a ideia de Estado-Nação do pós-Segunda Guerra Mundial não sobrevive alheia às crises internacionais, fazendo surgir uma nova ordem internacional com uma política externa incapaz de negar a tecnologia ou a importância que as redes sociais e o poder tecnológico têm na governação mundial atual. Sabemos que estamos perante uma modificação da ordem mundial, mas especular sobre qual e como será é muito incerto e ainda muito prematuro.

1.3. O impacto das Cidades Inteligentes para as Relações Internacionais

É cada vez mais evidente que um país politicamente poderoso é também um país em que existe um maior número de cidades inteligentes com tecnologia de ponta. Como tem sido recorrente nos últimos anos, os ataques cibernéticos são capazes de paralisar uma cidade e um país por completo, pelo que quem estiver mais bem preparado neste âmbito será, certamente, quem deterá o maior poder. No entanto, a facilidade nas transações digitais tem também impacto nas relações internacionais, não só nos seus desafios como também nos perigos que acarreta. Muito embora as vantagens da tecnologia sejam imensas, como descrito anteriormente, também é certo que existem muitos perigos e desafios associados, tanto na privação de dados, em termos pessoais, como nas ameaças no plano dos Estados.

Na verdade, o facto de as maiores cidades mundiais estarem cada vez mais dependentes do ciberespaço, traz uma série de fragilidades associadas como, por exemplo, a prevenção de ataques *hackers* que estão cada vez mais em voga e que tornam as cidades suscetíveis a ataques cibernéticos. Apesar de serem provocados à distância, nem por isso deixam de ser capazes de atingir as cidades a vários níveis, causando-lhes danos severos que, mesmo não sendo físicos (como a destruição da cidade ou baixas civis), põem em causa a segurança da cidade — por exemplo, bloqueio da comunicação, de contas bancárias, do sistema de saúde, etc. Além disso, existe também o risco de prevalecer uma nova forma de guerra que ultrapassa os ataques convencionais, uma vez que podem ser provocadas por um simples *click* capaz de pôr em causa a segurança de milhares de pessoas. Não só por serem à distância, mas também por não haver necessidade de enviar tropas do país atacante, o termo

guerras limpas surge para dar nome a um tipo de guerra que é acelerado pelo ciberespaço e que permite um maior controlo à distância de material bélico capaz de afetar países e cidades distantes, teoricamente com bastante precisão, e, por esse motivo, não provocando baixas em não combatentes e havendo uma redução considerável das áreas territoriais afetadas.

Efetivamente, o conceito de *ciberarmas* tem sido um termo bastante utilizado e referido por figuras políticas como Donald Trump que, numa entrevista a Sanger, admitiu estar disposto a recorrer à digitalização para atacar ou contra-atacar um Estado que interfira com a sua política, nomeadamente a Rússia — “Sanger: É favorável a os Estados Unidos não só desenvolverem mas usarem ciberarmas como alternativa a outras formas de defesa? / Trump: Sim. Eu sou fã do futuro, e o digital é o futuro”²⁴. Esta entrevista veio no sentido de confrontar Donald Trump com a sua estratégia perante uma eventual ação da Rússia ou da China, principalmente com o intuito de perceber a posição dos EUA na estratégia da NATO na eventualidade de a Rússia violar fronteiras de países membros, nomeadamente dos países do Báltico, ao que Trump se mostrou pouco cooperativo e sem nunca demonstrar uma posição inequívoca de apoio por parte dos EUA aos restantes Estados-membros da aliança militar. Esta posição é bastante reveladora não só do seu posicionamento político, mas também da sua opção por uma estratégia militar que abraça a digitalização de armas, uma estratégia que dá um passo na direção das *guerras limpas*, isto porque a utilização de ciberarmas permite que haja uma maior distância entre o país atacante e o país atacado. Mas que consequências podem estar associadas a esta operação? Certamente que deixa pendente alguns riscos associados a efeitos negativos, entre os quais uma tendência para a multiplicação e banalização do recurso à violência, isto porque a facilidade do envio de armas sem a necessidade do uso de tropas e o acesso rápido a este recurso acaba por retirar peso e significado à ação, tornando-a mais inconsciente. A isto fica ainda associada uma desumanização, no sentido em que não há tanta consciência das vidas que estão a ser postas em causa, por não haver contacto direto entre pessoas. Além disso, é também importante referir uma menor responsabilização política no recurso à violência, já que se torna muito mais tentador e fácil, tanto física como moralmente, passar para a violência com as ciberarmas. São mais imediatas, mais precisas no alvo, mais destrutivas, mais ameaçadoras, mas menos humanas no que toca à sua utilização. Este será, sem dúvida, o maior perigo:

²⁴ SANGER, David E. — **A Arma Perfeita: guerra, sabotagem e medo na Era da cibersegurança**, p. 261.

tornar-se muito fácil recorrer a este tipo de armamento sem pensar nas consequências e nas vidas que põe em causa.

Numa outra vertente, é passível de ser analisado o furto de dados pessoais, porque, de facto, com toda a nossa informação pessoal que circula constantemente na *internet*, é possível que a nossa privacidade seja comprometida em caso de um ataque cibernético. Além disso, hoje são conhecidos crimes de venda de informação e dados pessoais para fins de espionagens que comprometem a segurança da população e fomentam os perigos e desafios nas relações internacionais, uma vez que se torna bastante difícil o controlo destas atividades maliciosas. Por outro lado, a economia internacional também é afetada com a criação das criptomoedas, isto é, moedas digitais não controladas pelos Estados e que existem apenas no mundo virtual. Aliás, países mais conservadores e autoritários já proibiram a transação de criptomoedas precisamente pela falta de controlo que têm sobre as mesmas, o que tem impacto nas suas decisões políticas. Exemplos disso são a China e a Rússia, cujas ideologias políticas e práticas autoritárias facilitam a interdição destas transações — “A linha dura contra a criptomoeda encaixa-se com a posição dos poderosos serviços de segurança da Rússia, que também apoiam uma proibição de concorrência doméstica para impedir que ela seja usada para financiar a oposição do país, de acordo com duas pessoas familiarizadas com o assunto”²⁵.

O facto da tecnologia por detrás das criptomoedas ser o *blockchain*, isto é, uma tecnologia distributiva descentralizada, possibilita mitigar alguns riscos e tornar estas moedas digitais muito mais seguras, além de promover a inovação tecnológica. Embora estejam associadas a algumas atividades maliciosas, a verdade é que, por outro lado, as criptomoedas também são promovidas por bancos e investidores, sendo um mercado especulativo tão ativo como as ações, o que contribui ativamente para o crescimento da economia digital.

Em suma, a aceleração do mundo digital traz bastantes desafios para as relações internacionais, como irá ser mais detalhado adiante. É, por isso, crucial que haja um maior investimento na cibersegurança, para que, perante esta realidade, as pessoas possam permanecer seguras e com o seu direito à privacidade inalterado e protegido.

²⁵ Bloomberg — **Banco central da Rússia quer proibir mineração e comércio de criptomoedas** [Em linha]. Lisboa: Económico Valor, 2022.

1.4. A aceleração 5G

A tecnologia 5G é um fator relevante para o progresso das cidades inteligentes, uma vez que permite uma aceleração tecnológica, ou seja, o 5G é uma rede móvel de quinta geração mais rápida que as gerações anteriores e que, por isso, faz circular a informação instantaneamente. E, com uma *internet* mais rápida, torna-se mais apelativo o recurso à virtualização de vários serviços, à automação de automóveis, ao progresso da Indústria 5G e também ao recurso não só à Robótica como à Inteligência Artificial. Resumidamente, em todos os domínios públicos, coletivos e privados, toda a informação circula mais eficazmente e, por consequência, torna-se muito mais recorrente o uso deste recurso — “5G is a leap forward from its predecessor: its speed is up to 10 times faster than 4G; it has low latency, meaning there is only a minuscule delay of 1 to 1,000 milliseconds before a transfer of data begins following an instruction for its transfer; and it allows millions of Internet of Things (IoT) devices and sensors to be connected in a one kilometer square area — 4G only allows a limited number of connections”²⁶.

Neste sentido, o equipamento de cidades com tecnologia 5G foi acentuado com a situação pandémica vivida recentemente, abrindo espaço para a sua expansão, como foi já referido anteriormente. A *IoT* é uma realidade que surge com o 5G, não só porque a conectividade entre aparelhos e entre pessoas aumenta, como também porque começa a existir uma maior necessidade de que assim seja. De facto, a melhoria da vida da população faz com que haja uma maior adesão à *IoT* e, consequentemente, uma maior adesão ao desenvolvimento das cidades inteligentes.

Por outro lado, quanto mais atividades e aparelhos tivermos conectados à *internet*, mais fácil se torna a invasão de privacidade, pois o leque de possibilidades aumenta bastante. Apesar disso, é inevitável que os Estados se queiram associar a esta nova forma de sustentabilidade, aumentando, assim a “pegada digital” e, segundo João Borges e Teresa Rodrigues, “a *internet* beneficiou naturalmente desta aposta político-estratégica, assumindo-se como um dos principais vetores de suporte à designada «economia digital» e à própria governação dos Estados”²⁷. Indo ao encontro desta afirmação, a verdade é que as relações

²⁶ CARRIER, Op. cit.

²⁷ NUNES, Paulo — Ciberameaças e quadro legal dos conflitos no ciberespaço. In BORGES, João Vieira [et al.] — **Ameaças e Riscos Transnacionais no Novo Mundo Global**, p. 201.

internacionais estão envolvidas na capacidade de progresso dos Estados e no acompanhamento do que diz respeito também às novas estratégias políticas que, atualmente, estão bastante dependentes do ciberespaço.

Apesar de esta ser uma realidade que traz bastante conforto e vantagens a nível pessoal, a verdade é que a *IoT* acarreta também bastantes desafios, principalmente a nível das Relações Internacionais. Cada vez mais são criados *malwares* (*softwares* maliciosos, prejudiciais para os sistemas) com o intuito de penetrar os sistemas associados à *IoT*. Segundo um relatório apresentado pela Tech Monitor, os *hackers* estão a tornar-se cada vez mais sofisticados nestas manobras de invasão da *IoT*, mudando a sua estratégia e atacando primeiro as vítimas mais vulneráveis, ou seja, o utilizador comum²⁸.

A implementação da rede móvel 5G nas maiores cidades mundiais gera um progresso no desenvolvimento das próprias cidades inteligentes, uma vez que o espaço virtual se torna uma realidade muito presente na vida da população e da própria cidade. No entanto, é de salientar que o facto de a rede 5G não ter uma arquitetura tão centralizada aumenta as vulnerabilidades e o risco de ataques, pelo que é essencial que a sua implementação seja acompanhada por um avanço na cibersegurança.

Além disso, a nível económico e político, a rede 5G tem-se vindo a revelar como um fator relevante na corrida pelo domínio tecnológico: em 2020, os EUA pressionaram os seus aliados a banirem das suas estruturas de rede 5G o grupo chinês de telecomunicações Huawei, como reflexo das divergências políticas e económicas que já tinham vindo a crescer²⁹.

Em suma, o peso que a rede móvel 5G tem nas Relações Internacionais passa não só pelo domínio económico, mas também pela influência política. Embora o 5G traga efeitos positivos a nível do desenvolvimento das cidades, também apresenta desafios relativamente à segurança. Como foi possível analisar ao longo deste capítulo, decerto que uma cidade inteligente é muito mais do que apenas uma cidade digitalmente conectada. O impacto que tem, principalmente para as Relações Internacionais, envolve muito mais do que apenas o desenvolvimento económico. Reflete-se no poder económico do país e, consequentemente, na sua influência política a nível mundial. Analisar o desenvolvimento de uma cidade inteligente,

²⁸ MORRISON, Ryan — **Hackers increasingly targeting Internet of Things devices** [Em linha]. In Tech Monitor, 2022.

²⁹ DN/Lusa — **China condena pressão exercida pelos Estados Unidos sobre Portugal** [Em linha]. Lisboa: Diário de Notícias, 2020.

é também olhar para a posição que o país em questão tem no quadro mundial e a influência que exerce na definição da geopolítica atual. É possível olhar para este panorama e destacar a ação e o papel que países como a China e os EUA têm tido nos últimos tempos no que diz respeito ao equilíbrio (ou desequilíbrio) político mundial. Nas palavras de Scheider-Petsinger, esta é uma corrida que se tem vindo a acentuar também mediante uma corrida tecnológica que coloca os dois países numa luta pelo domínio financeiro a longo prazo — “China’s policies and practices related to technology transfer, IP and innovation are at the heart of the ongoing tariff escalation, which overshadowed the US and Chinese – and indeed global – economies in 2018 and 2019”³⁰. As estratégias adotadas por ambos os países são, por isso, em prol da diminuição dos países concorrentes, principalmente no domínio tecnológico, pelo que passam pelo surgimento de políticas no campo aeroespacial, da robótica, bem como da informação e comunicação tecnológica. Neste sentido, o rápido crescimento da China coloca em perigo a posição e domínio político dos EUA, não só pelos sucessos militares, como também pelos sucessos tecnológicos. Também segundo Hang (2017), o poder económico chinês é capaz de ditar significativamente o rumo político dos EUA, principalmente por ter deixado de ser visto como um país onde reina a pobreza para ser percebido como um país rico e uma das maiores economias mundiais — “Between 1981 and 2010, about 679 million of Chinese people were lifted above extreme poverty line. China is now seen as “the world’s largest economy (on a purchasing power parity basis) manufacturer, merchandise exporter and importer, and holder of foreign exchange reserves”³¹.

Assim, com a chegada do 5G todo este processo e esta definição de poder ganharam uma nova forma, uma vez que se tornou um domínio ambicionado por ambas as partes. Através do *soft power*, ou seja, a capacidade de influenciar outros países sem o recurso à força, a China tem conseguido entrar nos mercados mundiais e tem exercido uma forte influência no rumo das Relações Internacionais.

³⁰ SCHEIDER-PETSINGER, Marianne [*et al.*] — **US–China Strategic Competition. The Quest for Global Technological Leadership** [Em linha]. In Americas Programme, 2019.

³¹ Hang, N. T. T. — The Rise of China: Challenges, Implications, and Options for the United States. **Indian Journal of Asian Affairs** [Em linha]. 30:1/2, (2017), pp. 47–64.

Capítulo 2 | O direito à privacidade e à segurança

Com todas as vantagens associadas à *IoT*, a verdade é que, atualmente, toda a informação pessoal está bastante exposta ao perigo de invasão. Certamente que a maioria da população não está plenamente consciente deste perigo, não só pela falta de conhecimento, como também pela vulnerabilidade da informação partilhada.

De facto, sabemos hoje a importância que a cibersegurança tem na manutenção da privacidade de informação pessoal, muito embora a sua intervenção ainda se encontre muito aquém do expectável e daquilo que seria o ideal. Na verdade, a cibersegurança tem um custo demasiado elevado para aquilo que as pequenas e médias empresas consideram justificável e possível de investir, o que as leva a optarem, na sua maioria, por serviços mínimos que não estabelecem a visibilidade necessária sobre a *network*. Embora este cenário seja mais comum em empresas mais pequenas, também se verifica em empresas de maior dimensão. No entanto, e apesar de ser importante este investimento nas empresas, é nos Estados que deve ser feito o maior investimento, uma vez que são os maiores e mais diretos atores nas relações internacionais. A informação na posse dos Estados é tão sensível que uma falha no sistema estatal tem um impacto muito forte tanto a nível nacional como internacional, tornando o investimento em infra-estruturas de segurança imprescindível em todos os países.

No caso das empresas, os dados pessoais ficam vulneravelmente expostos a um ataque cibernético e é por isso também importante olhar para ataques recentes para compreender a dimensão que podem atingir. A título de exemplo, podemos analisar casos como o das empresas Cisco e Vodafone. Vejamos que no caso da empresa Vodafone, segundo a *press release* publicada no dia posterior ao ataque, dia 7 de fevereiro de 2022, a situação afetou “a prestação de serviços baseados em redes de dados, nomeadamente rede 4G/5G, serviços fixos de voz, televisão, SMS e serviços de atendimento voz/digital”³². Embora, nesta situação, haja a referência de que os dados dos clientes não foram afetados, a verdade é que a perturbação causada foi significativa, mesmo numa empresa que garante ter serviços e mecanismos de proteção contra este tipo de ataques. Segundo Bruno Duarte, *Senior Security Engineer* da Check Point, numa entrevista ao jornal IT Security “para mandar toda a infraestrutura de

³² Press Releases — **Vodafone Portugal alvo de ciberataque** [Em linha]. In Vodafone, 2022.

telemóvel e televisão abaixo, terá de ter sido um ataque de uma dimensão realmente grande, distribuído – com origem em vários sítios do globo, quase de certeza”³³.

Posteriormente, em maio de 2022, a Cisco, uma empresa direcionada para a tecnologia e que vende equipamentos e serviços relacionados com administração de sistemas, foi também alvo de um ciberataque com consequências graves para a privacidade de dados pessoais, uma vez que houve documentos da empresa que vieram a ser expostos na *darkweb*. Neste caso, ainda que os serviços não tenham sido diretamente afetados, um funcionário ficou com as suas credenciais comprometidas, tal como afirma o jornal IT Security — “a empresa descobriu que as credenciais de um funcionário foram comprometidas depois do atacante ter garantido o controlo de uma conta pessoal no Google”³⁴.

Quando dirigidos aos Estados as dimensões de ciberataques tomam proporções muito maiores. A título de exemplo, com a escalada dos ataques russos à Ucrânia, a cibersegurança enfrenta novos desafios, uma vez que houve um significativo aumento de ciberataques. Segundo um relatório da *Microsoft*, com a escalada da guerra da Rússia contra a Ucrânia, aumentaram também ataques entre outras nações, nomeadamente vindos do Irão contra os Estados Unidos da América e, inclusive, um aumento de ciberspionagem chinesa, principalmente contra os Estados Unidos da América³⁵.

Olhando para o primeiro ciberataque em grande escala conhecido, o ciberataque russo contra a Estónia em 2007, permitiu visualizar as dimensões que os ataques cibernéticos podem tomar. Como sabemos hoje, este foi, até ao momento, um dos ciberataques a uma nação com maior impacto, precisamente por aquilo que significou: a fragilidade das instituições estatais perante ataques cibernéticos vindos de outras nações. Esta série de ataques cibernéticos duraram quase três semanas e foram iniciados depois do governo ter anunciado a realocização da estátua do "Soldado de Bronze de Tallinn", que era vista como um símbolo da ocupação soviética — “For the local Russian minority it represents the

³³ DAMIÃO, Rui — **O que se sabe (até ao momento) sobre o ciberataque à Vodafone** [Em linha]. Lisboa: IT Security, 2022.

³⁴ Sem autor — **Cisco garante que ciberataque não impactou negócio e serviços** [Em linha]. In IT Security, 2022.

³⁵ Microsoft — **Ciberataques de Estado-nação se tornam mais ousados à medida que líderes autoritários escalam a agressão** [Em linha]. In Microsoft, 2022.

“liberator” while for the Estonians it represents the “oppressor””³⁶. Os ataques tiveram como alvo os *sites* de várias instituições da Estónia, incluindo bancos, agências governamentais e meios de comunicação. Estes ataques causaram interrupções e danos generalizados, tornando-se num dos ataques cibernéticos mais significativos da história moderna.

Os ataques cibernéticos começaram no dia 27 de abril de 2007 e continuaram até ao dia 18 de maio de 2007, tendo sido executados por um grande número de computadores que foram comprometidos por *hackers* usando um ataque distribuído de negação de serviço (DDoS³⁷). Este tipo de ataque é feito através da sobrecarga de um *site* com tráfego até que esse *site* se torne inacessível. Os invasores usaram *botnets*, isto é, redes de computadores infectados usados com o intuito de lançar os ataques DDoS³⁸.

O impacto destes ataques cibernéticos foi bastante significativo. Muitos *sites* do governo da Estónia ficaram *offline* por vários dias, causando interrupções nos serviços públicos. Os bancos também foram afetados, o que impediu as pessoas de acederem às suas contas *online*. Além disso, também os meios de comunicação foram alvo destes ataques, o que dificultou a cobertura dos acontecimentos. No seu conjunto, os ataques resultaram na perda de confiança na capacidade do governo da Estónia para proteger os seus cidadãos e as suas infraestruturas.

Quanto à resposta a este ataque, o governo da Estónia reagiu aos ataques com o apoio de parceiros internacionais para identificar a origem dos ataques e melhorar as suas medidas de segurança cibernética. Neste sentido, o governo criou uma Liga de Defesa Cibernética, uma organização voluntária composta por especialistas em segurança cibernética que trabalham para melhorar as infraestruturas de segurança cibernética da Estónia. Por outro lado, o governo estimou também focar-se em melhorar e fortalecer as suas relações com a NATO e com a União Europeia, que lhe forneceram apoio durante os ataques³⁹.

Por isso, o ataque cibernético da Estónia foi significativo não só porque foi um dos primeiros grandes ataques cibernéticos a atingir um Estado-Nação, mas também porque

³⁶ OTTIS, Rain — Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective [Em linha]. In OCCDCOE, 2008.

³⁷ *Distributed Denial of Service*, na sigla inglesa.

³⁸ Sem Autor — **2007 cyber attacks on Estonia** [Em linha]. In Cyber operations, sd. p. 54.

³⁹ HERZOG, Stephen — Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* [Em linha]. 4:2, Strategic Security in the Cyber Age (2011), p. 54.

destacou a vulnerabilidade dos países a ataques cibernéticos e a necessidade da criação de medidas robustas de segurança cibernética. Os ataques também levantaram questões sobre a aplicabilidade do direito internacional aos ataques cibernéticos e a necessidade de cooperação internacional para responder às ameaças cibernéticas. Um bom exemplo desta necessidade de cooperação foi a criação, em Tallin, da *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), um órgão que visa apoiar os países membros da NATO no domínio da investigação, formação e exercícios de cibersegurança abrangendo áreas como tecnologia, estratégia, operações e direito⁴⁰.

Este capítulo pretende, por isso, explorar o atual cenário da cibersegurança bem como os desafios que enfrenta, já que, como referido acima, as consequências de um ciberataque podem ser catastróficas e até grandes empresas com grande representatividade estão suscetíveis a este tipo de ameaça. De facto, muitos dos ataques são feitos a partir de várias zonas do mundo, tornando mais difícil a sua deteção.

2.1. A cibersegurança

A importância da cibersegurança tem vindo a crescer ao longo da última década e é este o conceito atribuído à Segurança que relaciona o universo cibernético e as redes de comunicação entre computadores⁴¹.

Efetivamente, a segurança de um país deve sempre acompanhar a evolução e caracterização das suas ameaças. Por isso, hoje em dia já não faz sentido falar em segurança sem falar em cibersegurança, uma vez que os ataques e as ofensivas são crescentemente executados através da *internet* e menos fisicamente. O que ainda se vê hoje em dia é a combinação destas duas vertentes, sem nunca excluir o reforço que o ciberespaço pode proporcionar a uma ofensiva física. Como foi referido no Capítulo 1, a aceleração da rede 5G veio trazer alguns novos desafios a nível da segurança e, portanto, a cibersegurança é cada vez mais necessária.

Uma das funções da cibersegurança passa também pela avaliação da gravidade dos ataques feitos a um sistema, uma vez que estes podem ser caracterizados em diferentes níveis, não só na sua motivação, mas também em função dos danos que poderão causar. O Instituto

⁴⁰ CCDCOE — **Our mission & Vision** [Em linha]. In CCDCOE, sd.

⁴¹ Dicionário Priberam. Entrada: *cibersegurança*.

de Defesa Nacional⁴² após considerar e analisar um eventual ataque considera que ele pode ser identificado como:

- **Ataque simples**, ou seja, um ataque que pode ser executado por uma ou mais pessoas, mas que não chegam a ser uma organização;
- **Ataque organizado**, onde já podemos encontrar um grupo organizado, tendo, por isso, um impacto maior do que um ataque simples;
- **Advanced Persistent Threats (APT)**, é um tipo de ataque que revela um maior conhecimento e uma maior precisão tecnológica, o que faz com que uma ameaça deste tipo seja muito maior, dado que é uma atividade maliciosa feita por profissionais e com um alvo específico;
- **Ataques coordenados de grande escala**, são ataques que tanto podem ser geridos por um grupo de pessoas como por uma Nação, o que os faz ter um impacto muito maior do que os anteriormente mencionados;
- **Ciberataques coordenados com ataques físicos**, são os ataques com o mais elevado nível de gravidade, já que correspondem a ataques feitos com recurso a diferentes dimensões, isto é, aéreo, marítimo e terrestre. Neste caso, o impacto causado é o mais elevado de todos e o que corresponde a um risco maior.

Estas categorias correspondem ao risco/gravidade dos ataques cibernéticos e são bastante relevantes para a Segurança Internacional pela sua dimensão internacional. Efetivamente, não se pode dissociar a segurança nacional da internacional, uma vez que um ataque a uma nação pode pôr em causa infraestruturas internacionais. Por isso mesmo, a defesa contra ciberataques deve ser feita de forma uniforme e cooperativa, tendo em conta o seu carácter global, por forma a garantir um ambiente seguro. Aliás, se o principal objetivo da Segurança Internacional é reduzir as ameaças entre nações, torna-se inevitável que se tenha em conta o tipo de ameaças referidas, acima de tudo porque são, maioritariamente, de cariz

⁴² IDN-CESEDEN — **Estratégia da Informação e Segurança no Ciberespaço** [Em linha]. In idn cadernos, 2013, p. 24-25.

internacional. Hoje em dia, um ciberataque vem de qualquer parte do mundo para quaisquer países, motivo pelo qual a Segurança Internacional deve estar atenta a estes fatores e agir em conformidade.

No entanto, no ciberespaço ainda podemos distinguir outro tipo de atividades que devem ser reguladas e controladas pela cibersegurança, como é o caso do cibercrime, da ciberespionagem e da ciberguerra. Todos estes conceitos são relativos a atividades maliciosas que estão em crescimento no ciberespaço e que hoje em dia são cada vez mais fáceis de executar devido à facilidade de acesso ao ciberespaço e ao constante avanço e aperfeiçoamento de dispositivos eletrónicos.

A nível das relações internacionais estes impactos também se fazem sentir. Na gestão de conflitos entre Estados, é importante referir que, segundo a Carta das Nações Unidas (1945) e o Convenção de Genebra (1949) — cujas funções são as de, respetivamente, legitimar o uso da força⁴³ e de conduzir os conflitos armados na perspetiva dos Direitos Humanos⁴⁴ —, estipulam o uso da força por parte de um Estado como um critério para constituição de um ataque. A nível cibernético estes critérios mantêm-se. No entanto, é importante perceber se uma ofensiva cibernética por parte de um Estado não visa disfarçar um mero ataque simples, ou até mesmo organizado, sobre o qual o Estado deseja descartar-se de responsabilidades. De facto, conhecer a causa e a origem de um ciberataque vai muito além de conseguir classificar o uso da força e já temos hoje conhecimento de casos onde, embora tenha sido possível prever que o ataque proveio da parte de um Estado, não foi possível prová-lo, o que faz persistir as especulações. Aliás, segundo João Borges (2017) o Manual de Tallin, um documento criado pelo órgão CCDCOE com o intuito de regulamentar a lei internacional na resolução de ciberconflitos, prevê que “o mero acolhimento oferecido por um Estado a um grupo que conduza operações no ciberespaço não pode ser considerado uso da força mas que, caso esse acolhimento seja acompanhado por um apoio claro e substancial, essa situação configura já um uso efetivo da força. [...] aponta oito critérios para ser possível identificar, de forma clara, uma situação deste tipo: severidade, imediatez, direcionamento, capacidade invasiva, mensurabilidade dos efeitos produzidos, caráter militar, envolvimento de Estados e presumível legalidade”⁴⁵.

⁴³ ONU — **Carta das Nações Unidas** [Em linha]. In ONU, sd.

⁴⁴ Ministério Público de Portugal — **Convenção de Genebra para melhorar a situação dos feridos e doentes das forças armadas em campanha** [Em linha]. Lisboa: Ministério Público, sd.

⁴⁵ BORGES, Op. cit, p. 209.

Deste modo, a classificação de ciberataques bem como a sua prevenção são parte crucial no processo de manutenção da paz internacional. Embora haja uma linha muito ténue entre que ataques podem ser da responsabilidade de um Estado ou não, a verdade é que é importante que haja uma linha condutora, uma vez que o ciberespaço faz parte da realidade e, portanto, do espaço físico de um país. Muitos dos problemas e das soluções atuais passam pelo ciberespaço e, por isso, a sua extensão ao mundo real deve ser controlada para que se tente colmatar o seu uso indevido. O Manual de Tallinn foi criado em 2013 com esse intuito após o ciberataque à Estónia em 2007. A título de exemplo, este caso, referido já anteriormente, terminou por não ser considerado como efetivo uso da força, uma vez que não teve consequências letais⁴⁶.

Importa também olhar para as camadas da *internet* que permitem um acesso e uso indevido do ciberespaço. Refira-se a própria *web*, que é mais controlada e onde há uma vigilância do conteúdo e das atividades que nela têm lugar, onde existe forma de, a partir de casa, conseguir aceder a este tipo de conteúdo e atividade. No que diz respeito aos níveis mais profundos da *internet*, embora todas as pessoas lhes possam aceder, nem toda a gente tem o conhecimento necessário para lá chegar e o seu acesso mais restrito também ajuda a que as atividades praticadas sejam muito mais difíceis de detetar e controlar, o que abre espaço para a prática de crimes graves como o tráfico humano, além de conter outros conteúdos violentos. A estas camadas dá-se o nome de *deepweb* e *darkweb*.

Quando nos referimos a conceitos como *deepweb* e a *darkweb*, referimo-nos a sítios ocultos da *internet* onde são comprados e vendidos todo o tipo de conteúdos, incluindo conteúdos ilegais, um mercado negro aos olhos da cibersegurança. Em termos técnicos, a *web*, utilizada por todos no dia a dia, corresponde apenas a uma primeira camada, a camada pública à qual alguns internautas gostam de chamar *The tip of the iceberg*.

Na camada seguinte, encontramos a *deepweb*. Aqui encontram-se dados de pessoas como senhas, *logins*, *emails* pessoais e já algum conteúdo que não deve ser de acesso comum, como informações confidenciais, registos médicos, dados de bancos, enfim, conteúdos que não põem em risco direto a vida das pessoas, mas que devem ser protegidos.

Por último, encontramos a *darkweb*, a última camada, cujo acesso requer muito mais conhecimento e perícia informática. Nesta camada, os donos dos *sites* ocultam o IP de modo a não serem nem identificados nem seguidos por ninguém e é por isso um ambiente propício à

⁴⁶ Idem.

ocorrência de atividades ilegais e às maiores e mais graves práticas criminosas que são um verdadeiro desafio para a cibersegurança, uma vez que são difíceis de regular e controlar.

O anonimato destas transações permite que a comunicação terrorista possa ser feita em fóruns fechados, o que facilita o planeamento destas atividades e incentiva vários atos terroristas a ganharem forma. A revista *Inspire*, por exemplo, foi criada pelo Al-Qaeda e é uma revista *online* propagandeada na *darkweb* que promove e compartilha táticas terroristas, como a oferta de orientação para criação de explosivos caseiros, incentivando assim ações e movimentos terroristas. Segundo Dziewanowski, em 2013 o ataque durante a maratona em Boston feito pelos irmãos Tsarnaev, foi inspirado por esta revista e existem provas recolhidas pelo *FBI* de documentos da *Inspire* encontrados nos seus computadores pessoais⁴⁷.

Por outro lado, na *darkweb* é também feito o recrutamento de indivíduos vulneráveis que são radicalizados para cometerem atos terroristas. Este recrutamento de pessoas de todo o mundo permite ampliar a cobertura das organizações terroristas transnacionais, por colocar em contacto recrutas de todas as partes do mundo. Neste sentido, o grupo Al-Qaeda, juntamente com outros grupos terroristas, incluindo o Daesh, utilizaram, numa primeira fase, a *darkweb* e as criptomoedas para financiar as suas atividades⁴⁸ e fizeram-no através de criação de doações fictícias em criptomoedas e, numa segunda fase, criaram uma criptomoeda com o intuito de absorver dinheiro de investidores privados.

Deste modo, é possível concluir que a *darkweb* tem um peso muito grande no terrorismo transnacional. É um dos meios mais favoráveis à sua propagação e permite que haja troca e roubo de informações usadas para fins criminosos. Os incentivos promovidos pela *darkweb* têm um impacto muito forte na forma de agir dos terroristas e hoje em dia é cada vez mais recorrente o recurso malicioso à *darkweb*, uma vez que é muito difícil detetar a propagação destes ideais e destas atividades criminosas.

No entanto, existem entidades que procuram dismantelar estas redes criminosas e perseguir a má conduta nas diversas camadas da *internet*. Na verdade, a Europol tem tentado travar este tipo de crimes cibernéticos nos últimos anos e recentemente, em setembro de 2023, a Europol foi capaz de demover um mercado negro *online* promovido na *darkweb* intitulado

⁴⁷ DZIEWANOWSKI, Jacek — AQAP Inspire Magazine as a tool motivating to terrorist activities. **Internal Security Review** [Em linha]. 20/10 (2019), p. 342.

⁴⁸ The United States Department of Justice — **Global Disruption of Three Terror Finance Cyber-Enabled Campaigns** [Em linha]. In Office of Public Affairs, 2020.

de *Piilopuoti* que tinha vindo a comercializar produtos ilegais desde maio de 2022⁴⁹. Além disso, a Europol tinha já conseguido também, em maio de 2023, detetar e inviabilizar negócios obscuros, dos quais faziam parte 288 pessoas de todo o mundo. Estes indivíduos estavam envolvidos na compra e venda de drogas e outros produtos ilícitos através da *darkweb*. Esta operação envolveu nove países (entre os quais Países Baixos, Alemanha, Brasil, EUA e Reino Unido) e teve a duração de 18 meses para que fosse possível apreender uma panóplia de bens ilícitos que estavam a ser comercializados⁵⁰. A necessidade de envolvimento destes países demonstra a importância da cooperação internacional, uma vez que sem este envolvimento e cooperação a operação poderia ter fracassado. A Deutsch News esclarece ainda que, nas palavras da Europol, na lista de vendedores e compradores estavam milhares de clientes por todo o mundo⁵¹. Neste sentido, pode-se também concluir que a cooperação internacional é essencial também pela dimensão destas atividades, isto é, não há fronteiras físicas nestes mercados negros e estes crimes revelam-se transnacionais, pelo que sem cooperação internacional será impossível deter crimes deste calibre. Este tipo de situações levam a crer que as instituições como a Europol são poucas. O crime liderado na *internet* está em crescimento pela facilidade e anonimato de que dispõem, pelo que os recursos de segurança devem ser incrementados e melhorados de modo a acompanharem este desenvolvimento.

Claro que, apesar destas conquistas, muitos crimes continuam a passar despercebidos, dado a dificuldade que há em conseguir sequer detetá-los. Sabe-se que existe venda de informação, tráfico de armas, tráfico humano, tráfico de droga, contratos homicidas, de terrorismo e muito mais. Em julho de 2023, na Holanda, um menino de 8 anos conseguiu, através da *darweb*, comprar uma arma AK-47 que lhe foi entregue à porta⁵². A facilidade com que uma criança conseguiu comprar uma arma sem levantar qualquer tipo de suspeitas, leva a crer que muito de negativo se passa neste meio tão extremamente indetetável.

Os dados pessoais também têm sido um alvo na *darkweb*. Segundo Schappert no cybernews (2023), um grupo de piratas informáticos foi detido em Amesterdão pelo roubo de

⁴⁹ Europol — **International operation closes down Piilopuoti dark web marketplace** [Em linha]. In Europol, 2023.

⁵⁰ Sem Autor — **International police arrest 288 worldwide in dark web bust** [Em linha]. In DutchNews, 2023.

⁵¹ Idem.

⁵² Prisha — **Eight-year-old boy orders an AK-47 from dark web, gets it delivered to home** [Em linha]. In Wion, 2023.

informação pessoal, mas, apesar da sua detenção, dados pessoais sensíveis continuam a circular pela *darkweb* para serem usados por outros cibercriminosos. Esta foi uma operação que durou dois anos, levando à detenção de três jovens que roubavam informação pessoal como nome, morada e número de telemóvel para pôr à venda na *darkweb*. O maior perigo encontra-se no roubo de informação mais sensível, como cartões de crédito, *passwords*, passaporte, entre outras⁵³. Tal como muitas operações na *darkweb*, o desmantelamento de organizações e grupos criminosos não invalida a continuação da circulação de produtos e de informação pessoal na *internet*. A maior dificuldade no combate ao cibercrime está, precisamente, na dificuldade em retirar da *internet* o que lá foi posto. Por essa razão, a simples detenção de criminosos não trava o crime em si.

Deste modo, importa aqui realçar que a *internet*, principalmente as camadas mais profundas, incentiva uma criminalidade muito difícil de combater e que não conhece barreiras físicas, pelo que a cooperação internacional é crucial para que possa ser combatido, de modo a precaver a segurança humana. Efetivamente, quando se fala em segurança humana podem ser mencionadas sete dimensões, segundo o Fundo Fiduciário das Nações Unidas para a Segurança Humana: a segurança económica, a segurança alimentar, a segurança na saúde, a segurança ambiental, a segurança pessoal, a segurança comunitária e, por fim, a segurança política⁵⁴. Adicionalmente, mais do que falar apenas nas dimensões da segurança humana, importa mencionar que surgem com o intuito de focar a segurança centrada nas pessoas e, por isso, orientada para a prevenção e proteção da população.

Relativamente às sete dimensões da segurança humana, é oportuno perceber até que ponto a tecnologia e as camadas da *internet* as podem pôr em causa. Para isso, e ainda segundo o Fundo Fiduciário das Nações Unidas para a Segurança Humana⁵⁵, descreve-se em seguida a definição de cada uma das dimensões da segurança humana:

- **segurança económica:** a segurança económica avalia-se pela pobreza persistente, pelo desemprego e por falta de oportunidades económicas. A segurança humana preza o combate à pobreza, uma vez que este é um fator de risco que gera fluxos

⁵³ SCHAPPERT, Stefanie — **Millions of personal data stolen by ethical hacker still floating around dark web** [Em linha]. In cybernews, 2023.

⁵⁴ United Nations — **Human Security Handbook. An integrated approach for the realization of the Sustainable Development Goals and the priority areas of the international community and the United Nations system** [Em linha]. In United Nations Trust Fund For Human Security, 2016, p. 7.

⁵⁵ Idem.

migratórios avultados e coloca em risco a vida das pessoas que vivem em condições miseráveis.

- **segurança alimentar:** corresponde à fome e aumento súbito do preço dos alimentos. O aumento da insegurança alimentar acresce o aumento da fome e subnutrição, pelo que é uma dimensão que muitas vezes está relacionada com a segurança económica e que culmina com a morte de milhares de pessoas e é, por isso, um fator importante e que está sob vigia das Nações Unidas.
- **segurança na saúde:** esta dimensão diz respeito às epidemias, à subnutrição e à falta de acesso a cuidados de saúde básicos. É certo que as epidemias são a causa de morte de muitas pessoas, principalmente nos países em desenvolvimento. O acesso a cuidados de saúde deve ser um fator assegurado a todas as pessoas e tem um valor incalculável, uma vez que pode prevenir inúmeras doenças e mortes prematuras.
- **segurança ambiental:** já a segurança ambiental define-se pela degradação ambiental, pelo esgotamento dos recursos naturais e pelas catástrofes naturais. Estes fatores têm sido recorrentes e uma constante e têm posto em causa a vida de milhares de pessoas. Preservar o planeta e combater este tipo de riscos é um plano urgente.
- **segurança pessoal:** desta dimensão faz parte a violência física, o tráfico de seres humanos e o trabalho infantil. Quando se fala em segurança, esta dimensão é aquela que tende a surgir em primeiro lugar, porque é, efetivamente, uma ofensa direta a um ser humano. A segurança preza pelo bem-estar das pessoas e, por isso, todo o tipo de ofensas deve ser vigiado e combatido.
- **segurança comunitária:** já a segurança comunitária diz respeito às tensões inter-étnicas, religiosas e de identidade que estão muitas vezes na origem da criminalidade e do terrorismo. Precaver este tipo de ações é crucial para a segurança humana.

- **segurança política:** por último, a dimensão da segurança política, corresponde à repressão política, à violação dos direitos humanos e à ausência do Estado de direito e de justiça.

Analisando as sete dimensões da segurança humana, pode-se concluir que o ciberespaço pode pôr em causa algumas delas, nomeadamente a segurança pessoal e a segurança política. De facto, enquanto a segurança económica, alimentar, na saúde e ambiental não são postas em causa ou fomentadas pelo manuseamento da *internet*, o mesmo já não acontece com a segurança pessoal, comunitária e política. Em termos de segurança pessoal, como já foi possível analisar, a *darkweb* possibilita e incentiva o tráfico de armas e de pessoas, mas também a contratação de serviços homicidas e ataques terroristas, pelo que se torna um desafio para a manutenção da segurança pessoal.

Por outro lado, a segurança comunitária também se vê desafiada pelo ciberespaço, uma vez que já existem inúmeros casos da difusão de ideias racistas e xenófobas a partir das redes sociais, como será alvo de análise mais adiante neste estudo. Embora as redes sociais como o Facebook e o Instagram tenham políticas que proíbem este tipo de comportamentos, a verdade é que não é possível combater esta propagação de ideais.

Por último, a segurança política também fica fragilizada. Como se verificou, a cibersegurança é uma área crucial para a manutenção de um ciberespaço seguro. No entanto, torna-se muito mais difícil para um Estado garantir a não violação de direitos humanos quando o direito à privacidade é colocado em causa.

2.2. A dificuldade na proteção de dados

No âmbito da proteção de dados, no final do ano de 2020, a Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e Política de Segurança apresentaram uma nova estratégia para a União Europeia com o intuito de proteger os cidadãos e os seus negócios das ameaças cibernéticas⁵⁶.

Nessa estratégia fixou-se que o principal objetivo da União Europeia diz respeito à adesão tecnológica e à segurança, tanto para o utilizador comum, como para entidades com informação mais cuidada e confidencial. A verdade é que nos últimos três anos houve um grande aumento na utilização da tecnologia, tendo em conta que este aumento foi mais

⁵⁶ European Commission — **The Cybersecurity Strategy** [Em linha]. Bruxelas: European Commission, 2022.

acentuado entre os anos 2020 e 2022 devido à situação pandémica do COVID-19, que obrigou ao refugio no digital, o que impulsionou uma forte evolução deste setor. Muito embora já houvesse uma tendência de grande progresso anterior a este momento, foi com o início da pandemia em 2020 que a necessidade de encontrar uma solução segura de convivência fez explodir o recurso à tecnologia. Desde o trabalho remoto até às compras *online*, tornou-se normal o uso do *online* para fins tanto de lazer como de trabalho, incluindo a realização de reuniões de alto nível político através do recurso à plataforma *Zoom*, entre outras.

Com o aumento de informação a circular no ciberespaço tornou-se obrigatório haver um acompanhamento da segurança na proteção de dados pessoais. No entanto, isto confirma-se como sendo um grande desafio, uma vez que a aceleração da tecnologia exige também uma evolução nos meios de segurança. Segundo a Comissão Europeia⁵⁷, existem três aspetos fulcrais a serem tratados:

1. **Resiliência:** ou seja, pretende-se tornar os sistemas de informação para, assim, aumentar a ciber resiliência de sistemas tanto públicos como privados. Estão, por isso, incluídos serviços como hospitais, redes de energia, laboratórios, centros de informação, etc. Ou seja, pretende-se tornar sistemas com informação sensível mais resilientes e protegidos de possíveis ameaças externas. Além disso, a Comissão Europeia pretende associar a estes objetivos a IA, a fim de detetar possíveis ataques muito mais cedo e, deste modo, prevenir a sua ação. Por último, é crucial que a tudo isto esteja associado a mão de obra especializada no domínio da cibersegurança.
2. **Capacidade operacional de prevenção:** no âmbito da prevenção, a Comissão Europeia está empenhada na criação de uma nova Unidade Cibernética Conjunta, isto é, num reforço da cooperação entre os organismos da União Europeia e as autoridades dos próprios Estados-membros. É nesta cooperação que fica assente uma maior capacidade de prevenção, uma vez que só assim se será mais fácil precaver um ciberataque e melhorar a ciberdefesa dos Estados-membros.
3. **Cooperação para um espaço cibernético global aberto:** um dos principais objetivos da Comissão Europeia é garantir a segurança e a estabilidade

⁵⁷ Idem.

internacionais no ciberespaço, bem como proteger os direitos humanos e as liberdades fundamentais. Neste sentido, a UE pretende investir fortemente na transição digital de países terceiros para que o reforço da cibersegurança seja muito mais amplo. Por fim, está nos planos da Comissão reforçar também as capacidades industriais e tecnológicas da UE, principalmente no que diz respeito à cibersegurança e, assim, impulsionar a sua autonomia estratégica, seja através de dados, da conectividade ultra-segura ou de redes 6G.

É, por isso, uma prioridade europeia o investimento, no período de sete anos, em equipamento tecnológico capaz de responder às ameaças inerentes a um ciberespaço aberto. O objetivo é que a segurança e proteção dos dados pessoais dos cidadãos não sejam comprometidos.

Efetivamente, o ataque a um país europeu pode comprometer toda a Europa. O facto de as cidades inteligentes crescerem e o uso da *internet* ser cada vez mais recorrente nas mais diversas atividades do dia a dia, faz com que este seja um ponto fraco de um país digitalmente desenvolvido, caso não se encontre devidamente protegido. Na realidade, uma cidade inteligente implica não só o acesso à tecnologia, mas também impõe que haja um acompanhamento deste avanço por parte de entidades estatais. Neste sentido, um país em que haja muitas cidades inteligentes vai automaticamente tornar-se um alvo maior de ataques cibernéticos, ou seja, o número de cidades inteligentes, sendo natural e desejável, implica também a necessidade de considerar complementarmente um conjunto de medidas de segurança.

Recentemente, existe um exemplo muito concreto em Portugal com dois ciberataques às Forças Armadas no espaço de um mês⁵⁸. Estes ataques expuseram a fragilidade do sistema da Defesa Nacional e colocaram em evidência a necessidade urgente de adotar serviços de proteção. A verdade é que o ataque às Forças Armadas portuguesas colocou em risco informação confidencial da NATO que, por sua vez, colocou em perigo todos os países membros. É, por isso, tão importante a proteção das infraestruturas internas das organizações nas relações internacionais.

A Comissão Europeia coloca um grande esforço e pressão em soluções uniformes e comuns a todos os países. Um ciberespaço exige respostas globais, mas será que a política

⁵⁸ MARCELINO, Valentina — **Ciberataques. "São mais um espelho da ineficácia da organização atual das Forças Armadas"** [Em linha]. Lisboa: Diário de Notícias, 2022.

européia e as suas divisões irão permitir esta uniformidade? Segundo a Comissão Europeia, o trabalho da ENISA⁵⁹ é reforçado com um trabalho permanente e vinculado à gestão de crises em toda a União Europeia, constituindo-se como uma entidade comum a todos os seus países com o intuito de uniformizar a segurança e a proteção da informação.

Além disso, é ainda referida uma certificação digital comum para que todos os produtos digitais a circular dentro da União Europeia possam ser válidos e de confiança. Ainda segundo a Comissão Europeia, grande parte da solução passa pela construção de produtos de confiança.

O aumento de ciberataques através de técnicas de *phishing*, isto é, através de técnicas que visam enganar usuários da *internet* de modo a obter informações confidenciais, como palavras-passe, dados pessoais, etc., implica outro grande risco difícil de controlar, isto porque são ataques que todos os dias chegam às caixas de correio eletrónico cada vez mais credíveis e bem estruturados. Este modelo de *phishing* mais comum é feito através do envio de *emails* ou SMS supostamente enviados por entidades credíveis, como bancos, seguradoras, clínicas, entre outras, onde influenciam os usuários a carregar em *links* que os levarão a fornecer informação pessoal. Por trás deste sistema estão *hackers* que controlam e roubam os dados que estão a ser inseridos.

De acordo com Eugenia Politou [*et al.*] (2018) num artigo publicado pela revista *Journal of Cybersecurity*, os termos *privacidade* e *proteção de dados pessoais* estão diretamente interligados, mas transmitem duas ideias diferentes⁶⁰. Enquanto a definição de privacidade se limita àquilo que é o espaço pessoal de cada indivíduo, a definição de dados pessoais refere-se àquilo que são os processamentos de dados relativos a um indivíduo. Em conjunto, ambos funcionam no sentido de proteger o espaço pessoal e segurança dos dados pessoais de cada indivíduo.

No que diz respeito ao ciberespaço, a maior dificuldade que surge é manter esta proteção num espaço em que a fragilidade na exposição destes dados é muito maior nos mais pequenos gestos de navegação na *internet*. A título de exemplo, atualmente todos os *websites* exigem a aceitação de *cookies*, ou seja, a aceitação da criação de um arquivo de informação sobre a atividade do utilizador no *website*: o tempo que está no *website*, o que procura, de onde faz a sua pesquisa, as suas preferências, entre outras informações. Autorizando as

⁵⁹ *European Union Agency for Cybersecurity*, na sigla inglesa.

⁶⁰ POLITOU, Eugenia [*et al.*] — Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. **Journal of Cybersecurity** [Em linha]. 4:1 (2018) p. 2.

cookies, da próxima vez que o mesmo utilizador entrar no *website* toda a informação já vai estar guardada e todos os produtos que pesquisou, os artigos que guardou no carrinho (mesmo sem sessão iniciada) vão estar exatamente onde os deixou e toda a informação do *website* vai estar direccionada para os interesses do utilizador. Por esse motivo, cada vez que se entra num *site* é necessário o consentimento de *HTTP*⁶¹ *cookies* e a verdade é que a maioria da população os aceita sem ter noção de que este consentimento permite a recolha e armazenamento de informação que regista todos os passos do utilizador.

Na realidade, o que estes *HTTP cookies* fazem é recolher a informação de navegação que está a ser criada pelo utilizador durante a sua pesquisa num determinado *site* e, além de recolher várias informações do dispositivo a ser utilizado na navegação, ainda pode recolher informações que estejam noutros dispositivos ligados à mesma rede. Resumidamente, ao aceitar *HTTP cookies*, o utilizador está a permitir que o *website* registe toda a sua atividade, localização e, muitas vezes, que aceda a informação guardada no dispositivo.

Embora existam vários tipos de *HTTP cookies* com diferentes finalidades (por exemplo de análise estatística, publicitária, de segurança...) a verdade é que muito poucas pessoas têm consciência de que estão a permitir este registo ao aceitá-las, tornando o perigo maior quando as aceita em *sites* pouco fidedignos, uma vez que existe a possibilidade de *hackers* infetarem computadores com vírus ou *malwares* recolherem informação pessoal e ainda seguir o registo histórico de navegação de forma maliciosa. Neste sentido, existem *cookies* de sessão e permanentes. A diferença entre estes dois é que o *cookie* de sessão é apagado quando o utilizador termina sessão, muito embora a informação guardada permita que haja uma restauração da sessão. Por outro lado, temos o *cookie* permanente onde a informação recolhida não é apagada com o fecho de sessão, mas sim ao fim de um tempo estipulado previamente pelo *website*. Embora correspondam a dois conceitos diferentes, a verdade é que ambos os *cookies* acabam por ser bastante parecidos e ser usados para o mesmo fim.

Simultaneamente, o aumento do volume das compras *online* e das subscrições que envolvem a inserção dos dados de conta bancária são também um risco. O maior desafio é o facto de todos os dados acima mencionados ficarem registados no ciberespaço, sem a possibilidade de serem removidos.

A exposição é imensa e enquanto já existe uma solução para a inserção de contas bancárias com a criação de cartões de compra única em aplicações como o MBWay, a verdade

⁶¹ *Hypertext Transfer Protocol*, na sigla inglesa.

é que no que diz respeito à navegação de um *site* existem alguns que não permitem que as *cookies* sejam rejeitadas, o que obriga as pessoas a aceitarem o registo caso queiram prosseguir com a sua pesquisa.

Assim, de modo a acompanhar os tempos que correm e a poupar tempo, as pessoas estão dispostas a depositar a sua confiança em terceiros para que possam aceitar os serviços, o que se torna um desafio ao qual a Comissão Europeia está já a tentar dar resposta com a criação de selos digitais e com certificações de segurança e credibilidade.

Um questionário⁶² realizado no âmbito desta investigação para perceber o nível de confiança que se coloca hoje em dia nas plataformas digitais comparativamente com o conhecimento que a população tem acerca das plataformas em que insere os dados, permitiu verificar resultados bastante impressionantes.

Num universo de 105 questionários realizados, em que cerca de 76% são jovens entre os 18 e os 24 anos, 65,7% recorrem à *internet* para a execução da sua atividade profissional e 32,4% recorrem algumas vezes, um fator bastante relevante que salienta a exposição que cada pessoa tem à *internet*, uma vez que se expõe não só a sua vida pessoal como também profissional.

No entanto, os dados mais interessantes surgem a seguir, quando apenas 1,9% admitiram ter um conhecimento muito baixo a nível informático, mas um total de 62% admitem saber o que são *HTTP Cookies* e para que servem⁶³. Depois, 87,6% admitem saber o que é a *darkweb* e a *deepweb*⁶⁴, mas 51,4% não sabem o que é o ciberespaço⁶⁵. Além disso, 17,1% não está consciente de que a sua informação pessoal pode circular no ciberespaço sem o seu consentimento⁶⁶. Estes dados são bastante reveladores para perceber se a população tem literacia informática e qual a divergência entre aquilo que julgam que sabem comparativamente àquilo que realmente sabem.

Ainda no âmbito das medidas de segurança que a população em causa tem tomado para que se possa proteger e evitar a divulgação dos seus dados pessoais de forma maliciosa, foi colocada uma questão sobre quais as medidas usadas para proteger a sua informação pessoal no ciberespaço. As quatro respostas mais vulgares consistiram na recusa de *cookies*

⁶² Ver Anexo 2.

⁶³ Idem.

⁶⁴ Ibidem.

⁶⁵ Ibidem.

⁶⁶ Ibidem.

não essenciais (61%), na conexão a *sites* considerados seguros (72,4%), no uso de plataformas sociais com comunicação encriptada sempre que possível (63,8%) e na não utilização de dispositivos de assistência virtual (55,2%)⁶⁷.

Relativamente às opiniões acerca da conexão digital de vários dispositivos eletrônicos verifica-se que divergem bastante, sendo que a que mais se distingue é a referência à sua utilidade e pragmatismo, muito embora haja opiniões em que, apesar do reconhecimento da utilidade, também receiam as consequências e impactos negativos que podem causar. Por outro lado, há quem admita que está consciente dos perigos, mas que perante a revolução tecnológica por que passamos não existe outra escolha além da de aceitar esses mesmos perigos e usufruir dos benefícios que a tecnologia nos traz. A insegurança e o desrespeito pela privacidade também são preocupações levantadas, no entanto também existem bastantes opiniões que privilegiam esta conexão por todas as facilidades que acarreta.

Em conclusão, 54,3% dos inquiridos receiam que a digitalização das atividades dos vários dispositivos do dia a dia coloque em risco a sua privacidade, 30,5% referem que talvez o receiem e 15,2% não o receiam de todo⁶⁸.

Este estudo foi bastante útil e pertinente para compreender não só qual a opinião dos utilizadores da *internet* acerca da evolução da tecnologia e qual a sua sensação de segurança, mas, principalmente, para conseguir perceber qual o nível de conhecimento que estes mesmos utilizadores têm em relação ao mundo tecnológico que os rodeia e de que forma isso pode estar relacionados com a sua consciência ou inconsciência acerca dos desafios que existem na proteção dos seus dados no espaço virtual.

Através da análise deste estudo podemos ainda tirar algumas conclusões, como por exemplo o modo como a inconsciência da população perante a partilha de dados pode influenciar diretamente as relações internacionais. Olhando para estes dados, é inevitável analisar a rede social TikTok que tem sido alvo de bastante controvérsia. Primeiro, porque, à data, já se sabe que esta rede social recolhia os dados pessoais dos utilizadores mesmo que estes não o autorizassem e, depois, porque existe a nível mundial uma elevada percentagem de pessoas a utilizar o TikTok, o que equivale à recolha em massa de dados pessoais.

No panorama global, esta acusação permite alavancar a tensão nas relações internacionais, uma vez que é fruto deste tema a acusação feita pelos EUA à China (dona

⁶⁷ Ibidem.

⁶⁸ Ibidem.

dessa rede social) de violação da legislação vigente no seu país⁶⁹. Resumidamente, os dados pessoais inseridos na rede social são motivo de conflito entre duas superpotências, o que só por si já revela o nível de importância que a proteção de dados pessoais na *internet* pode ter.

É, assim, evidente, a força política que hoje em dia as redes sociais podem ter, não só pela informação que detêm, mas também pela influência que conseguem ter nos próprios utilizadores. Embora não esteja preto no branco que a acusação norte-americana tenha fundamento, também é certo que esta está a ser uma consequência daquilo que as redes sociais representam na vida dos cidadãos e na prática política.

Um caso menos recente, mas ainda assim relevante, foi o caso do *Cambridge Analytica*, em 2014. Esta empresa londrina era uma empresa de consultadoria política que, como foi descoberto nesse mesmo ano, violou o direito de privacidade de mais de 50 milhões de utilizadores da rede social Facebook ao compilar os dados destes utilizadores de maneira a atingir os eleitores norte americanos aquando da campanha eleitoral, em 2016. Segundo o jornal *The Guardian*, a empresa *Cambridge Analytica* trabalhou com a equipa eleitoral de Donald Trump de modo a construir um programa de *software* capaz de prever e influenciar as escolhas nas urnas⁷⁰ e que culminou com a vitória de Trump e da sua tomada de posse em janeiro de 2017 — “We exploited Facebook to harvest millions of people’s profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on”⁷¹. Muito embora a recolha de dados pretendesse influenciar várias campanhas políticas em vários países, foi na campanha política de Donald Trump que teve o maior impacto.

Ainda segundo o jornal *The Guardian*, esta informação foi recolhida através de uma *app* que pedia aos utilizadores para fornecerem a sua informação pessoal a troco de dinheiro para um estudo universitário. O escândalo de *Cambridge Analytica* é dos mais conhecidos na atualidade, precisamente pela sua dimensão. Este esquema foi descoberto em 2018, quando Christopher Wylie, um ex consultor da empresa *Cambridge Analytica*, denunciou as práticas desta empresa à imprensa. A partir deste momento, o *CEO* do Facebook, Mark Zuckerberg foi, inclusive, convocado pelo próprio Congresso dos EUA e pelo Parlamento Europeu.

⁶⁹ Agência Lusa — **China garante que "nunca pediu" dados dos utilizadores do TikTok. E diz estar a ser alvo de “perseguição política alimentada pela xenofobia”** [Em linha]. Lisboa: CCN, 2023.

⁷⁰ CADWALLADR, Carole; GRAHAM-HARRISON, Emma — **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach** [Em linha]. Reino Unido: The Guardian, 2018.

⁷¹ Idem.

Assim, este caso de violação de dados privados deixou de ser um caso pontual de um único país e envolveu instituições políticas internacionais.

Como vimos, na era digital a vida política tem sofrido um grande impacto, principalmente nas campanhas eleitorais. Não se pode, por isso, deixar de mencionar um dos escândalos britânicos consequência da campanha eleitoral do referendo do *Brexit*, em 2016. Embora tenham acabado por serem determinadas como inconclusivas, de facto a empresa *Cambridge Analytica* foi alvo de investigações por se desconfiar que esta consultadoria política estava por trás de influência política ilegal nas redes sociais⁷².

No entanto, no caso do *Brexit* a história prolongou-se um pouco mais e as desconfianças de que as redes sociais estavam a ser usadas de forma abusiva chegaram à campanha *Vote Leave* por se desconfiar da utilização ilegal no financiamento de anúncios no Facebook para promover a campanha eleitoral junto dos britânicos⁷³. Embora ambas as situações não tenham sido comprovadas por falta de evidências, existem algumas conclusões que podem ser retiradas destas investigações. Notoriamente existe hoje em dia uma grande desconfiança política, principalmente no que diz respeito ao uso das redes sociais. O uso desta poderosa arma nas campanhas políticas deixa um rasto de desconfiança na disseminação de informação, uma vez que hoje em dia é um elemento chave para se chegar a uma vitória e por isso mesmo se torna tão apelativo usá-la de forma ilegal.

Aliás, embora a relação da vitória da campanha *Vote Leave* com a *Cambridge Analytica* e o uso de dinheiro ilegal da campanha em anúncios de Facebook se tenha mostrado inconclusiva, está já comprovado que o Facebook foi, de facto, usado como arma manipuladora durante todo o processo do referendo para o *Brexit*. Segundo o *The Guardian*, foi comprovado o uso de *bots*⁷⁴ para influenciar a opinião dos britânicos quanto à saída do Reino Unido da União Europeia. Neste caso, foram criadas, pouco tempo antes do referendo, centenas de contas de perfis de Facebook com fotos de perfil do partido favorável ao *Brexit*, onde foram partilhados, tanto no Facebook como no Twitter, centenas de vezes por dia e quase exclusivamente conteúdos sobre o *Brexit*⁷⁵. Ora, como sabemos, os algoritmos das

⁷² BALL, James — **The real story of Cambridge Analytica and Brexit** [Em linha]. Reino Unido: The Spectator, 2020.

⁷³ Idem.

⁷⁴ *Bot* é um diminutivo de *robot* e entende-se este conceito por ser um sistema de *software* criado para simular um humano, com ações repetidas e usando sempre o mesmo padrão.

⁷⁵ SAVAGE, Michael — **How Brexit party won Euro elections on social media – simple, negative messages to older voters** [Em linha]. In The Guardian, 2019.

redes sociais preveem que quanto mais um perfil publica e partilha, mais visibilidade tem. Estes *bots* ao partilharem consistentemente dezenas e centenas de vezes por dia tornam-se muito mais influentes e chegam a cada vez mais utilizadores. Psicologicamente, o facto de os utilizadores estarem constantemente a serem bombardeados com informação que promove o *Brexit*, acaba por influenciar muito a sua opinião.

Se agora compararmos as respostas ao questionário feito no âmbito deste estudo, é possível concluir e prever que a intuição da população é a de fornecer todo o tipo de dados que são pedidos e podemos agora relacionar a forma como esta atitude está a influenciar a política e as relações internacionais. A verdade é que a manipulação dos cidadãos através de redes sociais não é novidade e abre espaço para propaganda política com dimensões internacionais. No caso analisado, a empresa de consultadoria era britânica, mas servia interesses políticos norte americanos que, no caso, acabaram por favorecer a eleição de Donald Trump como presidente dos EUA.

Hoje em dia é cada vez mais recorrente haver este tipo de manipulação. De facto, é nas redes sociais que as pessoas passam mais tempo, fazendo dela um grande meio de influência, tanto política como social e é, por isso, recorrente o seu uso como meio de propaganda e influência.

Podemos, por isso, notar que as redes sociais têm vindo também a ter bastante influência na organização de manifestações violentas, como foi já referido anteriormente. A título de exemplo, a dimensão da invasão do Capitólio dos EUA e das manifestações violentas em Brasília foram uma consequência da disseminação destes ideais violentos nas redes sociais e que colocam em causa as dimensões da segurança pessoal e comunitária.

Contextualizando, a extrema direita norte americana organizou a invasão do Capitólio e moveu os apoiantes de Donald Trump através das redes sociais: partilhou informações como que ruas evitar, como desviar a polícia e, inclusive, houve pessoas a partilhar fotos a caminho do Capitólio a transportar armas, promovendo assim ainda mais a violência⁷⁶.

Já no caso brasileiro, em dezembro de 2022 os grupos extremistas apoiantes de Jair Bolsonaro iniciaram protestos e manifestações que foram também organizados através das redes sociais, primeiro por mensagens privadas em *apps* como o *WhatsApp* e *Telegram* e, posteriormente, para redes sociais com mais visibilidade. Para que a mobilização não fosse detetada, todo o protesto foi organizado sobre o código “Festa da Selma” e, tal como tinha

⁷⁶ FRENKEL, Sheera — **The storming of Capitol Hill was organized on social media** [Em linha]. In The New York Times, 2021.

acontecido com a invasão ao Capitólio, foram compartilhados vídeos e filmadas *lives* que transmitiam atos de violências, pessoas a vandalizar ruas e a incentivar outras a juntarem-se a estes protestos⁷⁷.

Em suma, os dados pessoais são muito sensíveis e suscetíveis de serem usados de forma abusiva, tanto em *websites* como nas redes sociais. Proteger estes dados e precaver a sua violação é um assunto que deve merecer bastante importância e atenção, porque, como foi possível analisar, o seu uso pode ter uma influência muito grande no comportamento e/ou manipulação das pessoas. A informação pessoal é uma arma muito poderosa para as relações internacionais e as redes sociais são cada vez mais um caminho para propagar ideais e comportamentos que, tanto podem ser positivos, como podem incentivar à violência e ao desrespeito pelo próximo.

⁷⁷ MALLERET, Constance; MILMO, Dan & HERN, Alex — **Pro-Bolsonaro violence: experts highlight role of social media platforms** [Em linha]. In The Guardian, 2023.

Capítulo 3 | Os casos de Londres e Amesterdão

Neste capítulo serão apresentados dois estudos de caso e será feita uma análise sobre o nível de desenvolvimento tecnológico das cidades de Londres e de Amesterdão. Que tipo de tecnologia utilizam e de que forma conseguem proteger as informações que circulam no espaço virtual, uma vez que este último é um fator inerente ao desenvolvimento da cidade no sentido de se tornar inteligente.

Além disso, neste capítulo também será abordada a maturação da segurança dos dados dos cidadãos, bem como as projeções que cada cidade tem para o futuro. Tendo em conta que não é possível olhar para um futuro sem tecnologia, é também importante perceber a ambição destas cidades em relação ao seu domínio tecnológico relativamente a outras grandes cidades mundiais e qual a sua posição no panorama internacional.

Consequentemente, será também analisado o impacto que os avanços destas duas cidades têm nas Relações Internacionais e a sua posição em relação a outros países.

3.1. O caso de Londres

A tecnologia tem, atualmente, um peso muito grande em Londres, principalmente no que diz respeito à conexão entre as pessoas e os serviços que presta com o objetivo de melhorar a qualidade de vida dos seus cidadãos. Hoje em dia, Londres conta com os mais diversos avanços tecnológicos, tais como Inteligência Artificial, realidade virtual e aumentada, rede 5G, forte adesão à *IoT*, robótica, automação de máquinas e tecnologias de contabilidade distribuída⁷⁸. Com a qualidade de vida dos cidadãos a aumentar a partir do recurso à IA, a verdade é que é possível estabelecer uma relação entre o desenvolvimento tecnológico e o aumento demográfico de Londres. Embora tenha havido uma tendência negativa, foi na viragem do século que a curva demográfica assumiu uma tendência positiva e em constante crescimento, coincidindo com a aposta tecnológica da cidade londrina⁷⁹.

Ao serem analisadas, estas tecnologias provam ser bastantes benéficas e existe, por isso, uma grande adesão à sua utilização, pelo que um dos grandes objetivos londrinos, definido pelo *Mayor* de Londres, Sadiq Khan, é conquistar a confiança das pessoas nestas

⁷⁸ YOUNG, Philip [*et al.*] — **London: A Global Leader in Advanced Digital Technologies** [Em linha]. In Catapult Digital, Londres, 2020, p. 5.

⁷⁹ Ver anexo 3.

tecnologias. Dando como primeiro exemplo a automação de veículos, está em curso um projeto que deteta a vulnerabilidade das pessoas e dos espaços em redor do veículo para que ele possa circular de forma automática e segura. Muito embora este cenário seja muito promissor, a verdade é que para que um veículo circule autonomamente de forma completamente segura, a população terá de se sujeitar às implicações inerentes a este processo. Como explica a empresa *Humanising Autonomy*, a sua pesquisa foca-se muito em conseguir prever todos os movimentos das pessoas em redor do veículo para que este consiga calcular o perigo e agir em conformidade⁸⁰. No entanto, é fácil prever que este *software* terá outras implicações a nível jurídico, isto porque, para que resulte, é essencial uma vigilância constante das pessoas no ambiente envolvente, que poderão nem estar conscientes deste estado de vigília. A título de exemplo, para que um veículo funcione automaticamente é necessário que haja uma recolha e transmissão de informação dos seus ocupantes, nomeadamente da sua localização e dos seus itinerários, estando sujeitos a serem intercetados por terceiros e podendo, assim, pôr em causa a privacidade destes passageiros.

Ainda relativamente à informação recolhida sobre estes passageiros, esta situação torna-se mais sensível quando a informação recolhida possa estar relacionada com membros do governo e do parlamento, diplomatas, militares e polícia de segurança. Na verdade, a informação sobre rotas e a localização de figuras políticas podem tornar este um problema mais grave e mais sensível, principalmente no que diz respeito ao cruzamento de leis entre países. Se estiverem em causa países da União Europeia será menos provável que haja um cruzamento de leis, uma vez que existe coesão e cooperação entre os Estados-Membros. Embora o Reino Unido já não faça parte da União Europeia, ainda mantém muitos critérios similares, como por exemplo, seguir a Regulamento Geral da Proteção de Dados⁸¹. No entanto, a circulação de dados pessoais vai muito além de países europeus, pelo que existe uma forte probabilidade de haver um conflito de interesses com países que seguem regulamentos diferentes.

Já no ecossistema digital é essencial a recolha do maior número de dados possível. Tendo em conta que a tecnologia visa servir pessoas, é necessário saber mais sobre essas mesmas pessoas, sobre as suas atividades diárias e sobre as suas preferências. Só assim é

⁸⁰ YOUNG, Op. cit, p. 10.

⁸¹ *GDPR — General Data Protection Regulation*, na sigla inglesa.

possível criar serviços que facilitem o seu quotidiano. Sendo Londres uma das cidades líderes globais em tecnologia, tanto os seus cidadãos como as próprias autoridades estão conscientes da relação inevitável entre a recolha de informação e o melhoramento de serviços, pelo que esta é uma cidade que trabalha todos os dias para uma recolha mais precisa e eficiente destes dados. Foram, inclusive, criados *softwares* capazes de recolher, tratar e transformar estes dados no produto final. Segundo o Mayor de Londres, Sadiq Khan, no Plano para Londres 2021, é essencial continua a investir nas infra-estruturas de conexão digital para que Londres não saia da corrida das maiorias cidades digitais do mundo⁸². Para o Reino Unido, o facto de Londres ser uma das cidades mais desenvolvidas a nível tecnológico coloca o país numa boa posição no quadro internacional, principalmente no plano económico. A aposta na tecnologia e em manter a cidade o mais desenvolvida possível é, por isso, um dos maiores objetivos expressos no plano apresentado em 2021, não só através do desenvolvimento de infra-estruturas, como também no acesso que as pessoas têm aos serviços digitais, certificando-se que os canais de fibra chegam a todos os usuários, ou suportando alternativas se ainda não for possível consegui-lo. Neste plano é ainda evidente que Londres, mais do que pretender ser neste domínio uma das principais cidades, procura ser líder no plano da conectividade digital⁸³.

De modo a manter o seu ritmo de crescimento, Londres tem ainda em vista quatro valores importantes⁸⁴:

- **Ser aberta:** a liberdade de comunicação entre pessoas e entre elas e as autoridades é um dos grandes objetivos. Fazem parte desta liberdade e partilha de pensamentos e opiniões num espaço livre e aberto a qualquer pessoa, permitindo assim a inclusão social sem nunca pôr de parte a segurança e a proteção de dados.
- **Respeitar a diversidade:** uma grande ambição para Londres é também estar suficientemente equipada para que possa concorrer e até superar outras cidades

⁸² Greater London Authority — **The Spatial Development Strategy For Greater London** [Em linha]. Londres: The London Plan, 2021, p. 361.

⁸³ Idem, p. 362.

⁸⁴ Mayor Of London — **An Emerging Technology Charter for London** [Em linha]. Londres, 2021, atual. fevereiro 2022.

européias e norte-americanas. Uma imagem global onde a tecnologia impera nunca poderá funcionar sem a colaboração de todos os países, respeitando sempre as culturas e normas de cada um. Este é um dos pontos mais fulcrais a ter em conta no que diz respeito ao papel que as cidades inteligentes têm nas Relações Internacionais.

- **Ser confiável no que diz respeito aos dados das pessoas:** um dos pontos mais debatidos nesta investigação é a questão dos direitos dos utilizadores da *internet*, principalmente no que diz respeito ao direito à privacidade. Sendo Londres uma cidade democrática nunca coloca de parte esta questão tão importante e esforça-se no sentido de manter os dados dos seus cidadãos o mais protegidos possível. Mas será que estão a fazer o suficiente? Muito embora o governo britânico esteja consciente da importância da defesa dos direitos de privacidade, o trabalho que tem desenvolvido ainda se mostra insuficiente na relação entre aquilo que a cibersegurança deve alcançar e que aquilo que de facto consegue atingir — “The level of maturity, capability, investment, and security understanding across government organisations remains inconsistent and the size and complexity of government’s digital estate, including the presence of legacy IT, makes the challenge significantly more complicated”⁸⁵.
- **Ser sustentável:** sendo a diminuição da pegada ecológica tão importante, é essencial que a tecnologia seja o mais sustentável possível e que contribua para a economização de espaços e opções mais sustentáveis.

Olhando para o atual crescimento digital de Londres, podemos considerar outras regiões que já ultrapassaram esta fasquia para que seja possível analisar a perspetiva do caminho que Londres está a querer seguir ou que poderá tomar. Por exemplo, Taiwan está já num ponto de partida bastante avançado e a verdade é que ainda há um grande caminho a percorrer para que Londres se possa equiparar à capital de Taiwan, Taipé, onde a indústria automóvel e os transportes públicos estão a ser alvos de grandes investimentos, apostando

⁸⁵ HM Government — **Government Cyber Security Strategy: Building a cyber resilient public sector** [Em linha]. Londres: HM Government, sd, p. 15.

cada vez mais na digitalização e automação deste setor. Por exemplo, segundo um artigo publicado por *Hive Life*, até 2025 estão previstos serem investidos cerca de 200 milhões de dólares nos transportes, não só nos serviços que prestam, mas também na recolha de informação para que seja possível saber de antemão o nível de tráfego e a disponibilidade de estacionamento⁸⁶.

Embora Londres ainda não esteja neste nível de avanço tecnológico neste setor, é certo que o setor automóvel e dos transportes públicos é alvo de grandes investimentos. Em comparação, e sendo Taipé uma cidade inteligente mais desenvolvida, Londres parece percorrer também este caminho que culminará numa maior automação. Por exemplo, Londres já utiliza uma tecnologia de iluminação pública inteligente, o que também já é uma realidade em Taipé. Esta tecnologia em Taipé usa as fontes renováveis e dispositivos de gestão inteligente na distribuição de energia. Aliada à telemedicina, à construção de centros de controlo e operações (como câmaras de vigilância de alta tecnologia), a plataformas de *e-learning* e, principalmente, à adesão a parques eletrónicos e infra-estruturas de telecomunicação para a segurança e gestão de dados públicos⁸⁷, existe em Taipé uma inovação tecnológica muito mais avançada do que aquilo que se vê na Europa. No entanto, também são visíveis os sinais de mudança e de crescimento nas mesmas linhas de evolução de Taipé.

Ainda assim, Taipé não está isolado e tenta abrir-se a outros países através da cooperação internacional, nomeadamente através do Fórum Internacional das Cidades Inteligentes que já realizou em 2023 a sua quarta conferência. Neste Fórum participam instituições académicas e de investigação nas mais variadas indústrias pertencentes a países como os EUA, o Canadá, a Austrália, Áustria e Taiwan⁸⁸. Segundo as ideias discutidas neste Fórum, a Nova Taipé é a maior cidade de Taiwan que visa pôr em prática todas as iniciativas que incorporem tecnologia de ponta, nomeadamente a IA e, por isso, criaram projetos como o *Big Data Center* ou, por outras palavras, uma rede de computadores, de sistemas de armazenamento e de infraestruturas computacionais que organizam, armazenam e disseminam

⁸⁶ CHIN, Bernice — **Inside Smart City Taiwan: A New Solution for Urban Living** [Em linha]. Taiwan: Hive Live, 2021.

⁸⁷ Bright Cities — **Mapa Mundial de cidades inteligentes: Taipei** [Em linha]. In Bright Cities, sd.

⁸⁸ Sem autor — **Smart City-2023 NTPC International Smart City Forum** [Em linha]. In Smart New Taipei City, 2023.

grandes quantidades de informação⁸⁹, ou seja, Taipé já começou e continua a criar infraestruturas capazes de recolher, analisar e processar grandes quantidades de informação para que seja viável o desenvolvimento de infraestruturas de resposta às necessidades dos seus habitantes. A título de exemplo, Taiwan criou um sistema de pagamento virtual — the *New Taipei Mobile Payment APP (NewTaiPAY)* — que recompensa os utilizadores com moedas virtuais aquando da sua utilização e prevê no futuro a introdução de descontos, obtenção e transferência de pontos, etc⁹⁰. Claro que com esta aplicação será essencial o reforço da segurança das transações, bem como da proteção dos dados pessoais que circulam neste espaço.

A título de comparação, Tóquio, a capital japonesa, parece também focar-se bastante no desenvolvimento e crescimento enquanto cidade inteligente. Na verdade, no Japão as cidades inteligentes foram mesmo consideradas como a solução mais eficiente para os problemas atuais e futuros. Por isso, tanto empresas, como universidades e setores públicos já se juntaram ao *Smart City Institute Japan*, que conta não só com a presença de empresas japonesas, mas também com empresas internacionais que olham para o Japão como um líder mundial no plano tecnológico⁹¹.

Neste patamar de desenvolvimento é também crucial referir o tipo de *backlog* utilizado, isto é, o histórico da informação e a forma como é recolhida e analisada. Tendo em conta que a tecnologia deve visar servir o ser humano é inevitável que haja um estudo e registo dos seus comportamentos e uma análise de informações recolhidas relativamente às suas necessidades.

Este registo não pode deixar de ser feito. No entanto existem várias formas de o fazer. Se por um lado esta informação pode ser registada, analisada, posta em prática e eliminada, por outra ela pode ficar armazenada mesmo depois de ter sido analisada. Na verdade, Londres está abrangida pelo *The Human Rights Act* ⁹² que inclusive abrange o direito à privacidade da informação pessoal, incluindo fotografias tiradas sem o consentimento do cidadão — “respect

⁸⁹ YASAR, Kinza; LOSHIN, Peter; LUTKEVICH, Ben — **Definition data center** [Em linha]. In TechTarget, 2022.

⁹⁰ Sem autor — **New Taipei mobile payment (NewTaiPAY) combined with New Taipei coin will be launched in July** [Em linha]. In Smart New Taipei City, 2023.

⁹¹ REGAN, Emma — **Smart Cities in Japan: Practical Innovations for Conscious Future Living** [Em linha]. In Tokyoosque, 2022.

⁹² I. Iberty — **The Human Rights Act** [Em linha]. Londres: I. Iberty, 2022.

for your private life and confidential information, including the story storing and sharing of data about you” e “the right to control the spreading of Information about your private Life, including photographs taken covertly”⁹³. Neste sentido, o tipo de *backlog* usado não pode, de forma alguma, ir contra estes princípios. No entanto, será possível haver uma evolução dos sistemas sem violar estas normas? De facto, será sempre necessário haver uma recolha de dados para estudar os comportamentos de cada indivíduo, como é exemplo a automação. Tendo em conta que a evolução da automação vem no seguimento do estudo do indivíduo e da recolha de dados factuais, como poderá haver uma evolução sem a invasão da privacidade individual?

Neste momento, o facto de o Reino Unido não fazer parte da União Europeia leva a que não tenham de seguir as suas leis, regulamentos e diretivas. Por isso, para que a segurança na proteção de dados consiga acompanhar a evolução tecnológica é essencial que haja boas infra-estruturas capazes de dar resposta a ameaças. Em boa verdade, o Reino Unido mantém uma boa relação funcional com a ENISA, já que preveem incorporar os princípios fundamentais de proteção de dados pessoais, maximizando a sua segurança e capacitando os indivíduos. Esta proteção de dados pessoais também se aplica em caso de transferências internacionais se o indivíduo pretender transferir esta informação para países terceiros⁹⁴.

Atualmente, Londres continua a trabalhar para conseguir manter a sua posição a nível internacional, tentando sempre acompanhar o avanço tecnológico. Neste momento já há perspectivas para a evolução da computação quântica e de interfaces cérebro-computador⁹⁵. Em rigor, por computação quântica entende-se uma supercomputação capaz de armazenar um elevado número de informação. Neste momento, a tecnologia em curso começa a mostrar sinais de lentidão, com baixa capacidade de armazenamento e com uma capacidade insuficiente para realizar operações matemáticas complexas. Podemos dizer que se chegou a um ponto em que esta tecnologia paralisou no tamanho mínimo físico que pode atingir e esta estagnação obrigou à necessidade de procura por capacidades computacionais do *hardware* atual, ou seja, entrámos na computação quântica. A computação é, então, associada à mecânica quântica que se debruça no estudo de partículas atómicas e subatómicas e o

⁹³ I. Liberty — **A Private and Family Life** [Em linha]. Londres: I. Liberty, 2022.

⁹⁴ Information Commissioner’s Office — **Data Protection by design and default** [Em linha]. In Information Commissioner’s Office, sd.

⁹⁵ Mayor of London, Op. cit, p. 5.

desenvolvimento deste novo tipo de tecnologia é, neste momento, um dos setores mais relevantes no mundo digital. Os efeitos da descoberta e aplicação da computação quântica cria uma competição global muito forte, pelo que o Reino Unido está empenhado no investimento neste setor, sendo que atualmente são a China e os EUA que dominam o setor — “Ministers are to launch a 10-year programme to invest £2.5bn in quantum computing, aiming to keep the UK competitive in one of the world’s fastest moving fields of technology”⁹⁶.

Apesar dos esforços britânicos e norte americanos, atualmente a China lidera a computação quântica, uma vez que já conseguiu testar um computador quântico, assumindo a liderança nesta corrida. Com protótipos a ser testados há seis anos, a China consegue agora montar um sistema de computação quântica vinculado a uma *cloud* que se pretende que seja acessível, primeiro, a instituições e, posteriormente, abranja a população em geral⁹⁷. A capacidade deste tipo de tecnologia ainda está a ser estudada, numa tentativa de prever e equacionar o impacto do futuro dos meios envolventes.

A computação quântica tem uma vasta quantidade de benefícios no que diz respeito à ciência (nomeadamente na procura de curas para doenças), à física, ao desporto e até mesmo à política. Estes cenários resultam da quantidade de dados viáveis de serem inseridos num sistema, suficientes para ser possível reproduzir milhões de testes e verificar numa questão de segundos a possibilidade de um determinado comportamento. No entanto, trará também muitas outras questões que farão com que a atual tecnologia não a consiga acompanhar, pelo menos nos moldes em que se encontra nesta fase transitória. De facto, com a capacidade dos computadores quânticos de detetar e criar novos mecanismos, será possível acelerar a medicina e, segundo Michio Kaku (2023), professor de física teórica, “Em vez de perder muito tempo a experimentar diferentes substâncias ao longo de muitas décadas, talvez consigamos criar rapidamente novos medicamentos na memória de um computador quântico”⁹⁸. Ainda segundo Michio Kaku (2023), com a computação quântica é possível utilizar sensores que detetam odores emitidos pelas células cancerígenas e refere que eventualmente no futuro será possível conectá-los a um computador quântico para que este possa analisar os odores e detetar o tipo

⁹⁶ COOKSON, Clive; PARKER, George — **UK to invest £2.5bn in quantum computing drive** [Em linha]. Reino Unido: Financial Times, 2023.

⁹⁷ XINHUA — **East China lab to get world-leading quantum computer** [Em linha]. In China Daily, 2023.

⁹⁸ KAKU, Michio — **Supremacia Quântica**, p. 175.

de cancro ao mesmo tempo que o trava⁹⁹. A descoberta para a cura contra o cancro é eminente e encontra-se à distância do recurso à computação quântica. Hoje em dia já é evidente que é possível encontrar a cura para esta doença que tem feito sofrer tantas pessoas, consequência da revolução tecnológica. Por outro lado, se a IA associada a computadores digitais já tem resultados bastante relevantes, embora encontre muitas limitações, quando associada à computação quântica os resultados são alavancados de uma forma exorbitante. Por exemplo, a IA tem a capacidade de aprender coisas novas, no entanto, os computadores digitais não têm a capacidade de compreender e executar todas as tarefas aprendidas pela IA, porque são bastante limitados. O mesmo não acontece com a computação quântica, que tem potência suficiente para executar todas as tarefas aprendidas pela IA, sem qualquer limite. Assim, juntam-se duas tecnologia que se complementam uma com a outra sem se limitarem: a IA aprende e a computação quântica executa¹⁰⁰.

Além disso, a vantagem da computação quântica também se torna evidente na operação de satélites dotados com este tipo de tecnologia, tendo em conta que permite que haja uma comunicação mais rápida, segura e eficaz entre o espaço e a Terra.

Por outro lado, os cientistas chineses projetam também radares providos de tecnologia quântica capazes de penetrar tecnologias militares, principalmente norte americanas, e detetar os submarinos tecnologicamente mais sofisticados no presente¹⁰¹. O facto de a China ter esta vantagem sobre os EUA reflete muito do poder que a China detém neste momento e valoriza a sua posição a nível internacional. De facto, atualmente, já se fala numa segunda Guerra Fria, não só por todas as tensões geradas em torno da guerra da Ucrânia, mas também por uma rivalidade que tem vindo a crescer nos últimos anos entre os EUA e a China e em que a liderança tecnológica assume um dos papéis principais. Como referido no Capítulo 1 do presente estudo, a nova ordem mundial está também a ser definida pela tecnologia e pelo seu domínio, pelo que a computação quântica se revela um fator crucial nesta crescente tensão.

É, por isso, importante perceber qual o impacto a nível internacional que este avanço pode ter. Por um lado, quando a informação circula no ciberespaço é transmitida de forma encriptada, isto é, para que circule de forma mais segura, a informação é protegida por um

⁹⁹ Idem, p. 190.

¹⁰⁰ Ibidem, p. 207.

¹⁰¹ HOWELL, Sam — **The China-US Quantum Race: In the quantum race, second place may be the first to lose** [Em linha]. In The Diplomat, 2023.

código que só pode ser desbloqueado por uma chave digital única à qual apenas o destinatário tem acesso. Desta forma, a informação pode circular no ciberespaço sem ser roubada ou alterada e, caso esta informação seja interceptada, apenas vão estar visíveis um conjunto de caracteres anónimos. No entanto, a computação quântica vem alterar esta forma de encriptação de dados, uma vez que tem a capacidade de descodificar este código em segundos, o que deixa a informação bastante vulnerável.

A nível internacional este avanço tecnológico tem muito impacto, uma vez que no ciberespaço não circula apenas informação pessoal dos cidadãos, mas também informação de cariz militar e dos próprios Estados. Pensar que esta informação se torna mais vulnerável tem um impacto muito grande na forma como se olha para a computação quântica no quadro internacional.

Já em relação à interface cérebro-computador estamos perante uma tecnologia de colaboração entre o cérebro humano e o computador, em que o cérebro consegue delegar arbitrariamente tarefas a dispositivos que as vão executar. Muito embora ainda haja um grande caminho a percorrer, este tipo de avanços já são uma realidade e já estão no horizonte de um futuro próximo. O impacto deste desenvolvimento tem um grande peso no poder internacional, uma vez que a relação entre a utilização do cérebro humano com a precisão da execução robótica tanto pode trazer imensos benefícios e trabalhar a favor da população e dos Estados, como pode ser usada maliciosamente, pondo em causa a sua segurança, já que o acesso a informação sensível fica bastante vulnerável. Além disso, a competição económica é também um fator de peso na concorrência internacional, tendo em conta que esta tecnologia de ponta é o reflexo de um grande investimento na ciência e na tecnologia, refletindo, por sua vez, o poder de um Estado, tanto pela sua capacidade económica e avanço científico, como pelo tipo de tecnologia que passa a dominar e que tem agora em seu poder. Neste sentido, Londres mantém um grande interesse neste domínio e direciona parte do seu orçamento para a ciência e tecnologia, procurando traçar o seu caminho no contexto do setor tecnológico.

Percebendo a posição da China e do Reino Unido, é interessante olhar também para uma cidade norte-americana e, deste modo, compará-la com o que está a acontecer na Europa e na Ásia. Tendo em conta esta ordem de ideias, também a capital americana conta já com um conjunto de diretrizes para se desenvolver enquanto cidade inteligente. A título de exemplo, e segundo Morningstar (2021), Washington D.C. tem vindo a promover algumas iniciativas

como a substituição de postes de rua por iluminação pública inteligente — esta iniciativa visa a poupança de energia, uma vez que as luzes LED acendem consoante o movimento —; a instalação de quiosques digitais, com WI-FI gratuito e serviços de orientação e informação; a criação de uma plataforma de partilha de dados, com o intuito de recolher e analisar dados para que possa ser entregue à população um serviço mais personalizado e de acordo com as suas necessidades e preferências, ao mesmo tempo que a ajuda a tomar decisões mais informadas. Esta plataforma pode recolher dados de várias fontes, como por exemplo sobre transportes públicos, sensores ambientais e serviços de emergência. Além disso, desde 2019 que está também em vigor o transporte autónomo, isto é, vaivéns autónomos que transportam pessoas e que desde então têm comprovado a eficiência na autonomia dos transportes, uma vez que o congestionamento de trânsito fica bastante reduzido. Importa ainda referir que a cidade tem vindo a implementar um sistema inteligente de gestão de resíduos para que seja possível monitorizar os contentores da cidade e, assim, otimizar a recolha do lixo¹⁰².

Ainda assim, muito embora a capital americana esteja a acompanhar as diretrizes de uma cidade inteligente, Londres continua com objetivos mais desafiantes e com um foco muito maior no desenvolvimento tecnológico do espaço citadino. As infraestruturas têm uma tecnologia muito mais avançada e os objetivos são muito mais ambiciosos.

3.2. O caso de Amesterdão

Amesterdão é hoje um líder global no desenvolvimento e nas estratégias de cidades inteligentes na Europa, tendo já inúmeros sistemas que o definem e que contribuem para o seu avanço tecnológico. Tal como é recorrente em todas as cidades inteligentes, a inclusão social e o aumento da qualidade de vida são fatores essenciais para as suas estratégias de desenvolvimento e esse aumento da qualidade de vida acabou por se refletir no aumento demográfico desta cidade inteligente. Efetivamente, de 2009 a 2022, o crescimento demográfico de Amesterdão tem sido visível tendo, em 2022, atingido o valor demográfico mais alto desde 2009 e a tendência no decorrer desses anos foi sempre positiva, nunca tendo tido uma regressão¹⁰³.

¹⁰² MORNINGSTAR, Murohy — **Washington** [Em linha]. In About Smart Cities, 2021.

¹⁰³ Ver anexo 4.

A verdade é que os holandeses sempre foram um povo conhecido pelas suas políticas mais liberais e pela sua forma de vida mais descontraída, um conjunto de fatores que, em última instância, são bastante favoráveis para a aplicação de novas tecnologias no dia a dia, ainda que reconheçam que são potenciadoras de algumas vulnerabilidades. Falando sobre exemplos de alguns objetivos desta estratégia digital, os Países Baixos estão a apostar na digitalização do governo, para que se torne mais transparente e acessível; na educação, de modo a incrementar a qualidade do ensino; na saúde, com a melhoria da qualidade de vida em vista com este investimento; na agricultura, de modo a torná-la mais sustentável; na mobilidade, com carros inteligentes e, consequentemente, mais sustentáveis; e nos setores da energia e da indústria, para se tornem mais flexíveis¹⁰⁴. Este modo de vida aliado a uma forte colaboração por parte do Estado na implementação de novas estratégias culmina numa postura holandesa muito forte no que diz respeito a cidades inteligentes. À escala internacional, Amesterdão ganhou o prémio *iCapital* em 2016, um prémio atribuído pela Comissão Europeia que visa o reconhecimento das cidades europeias que mais contribuem para promoção e inovação das suas cidades¹⁰⁵.

Enquanto todas as cidades têm uma estratégia própria definida para se desenvolverem enquanto cidades inteligentes, Amesterdão regula-se bastante em torno daquilo que são os objetivos de sustentabilidade estabelecidos pela Comissão Europeia, principalmente no que diz respeito a energias limpas. De facto, até 2030 a Comissão Europeia definiu já o impacto que as energias não renováveis têm no planeta e a urgência na redução destas emissões — comparado com 1990, o objetivo é reduzir a emissão de gases em, pelo menos, 40% até 2030¹⁰⁶. Amesterdão foca, por isso, os seus objetivos nas metas da própria União Europeia, nomeadamente no aumento da eficiência energética e na redução das emissões de CO₂¹⁰⁷. Este plano está a ser posto em prática através do incentivo de utilização de painéis solares e turbinas eólicas.

¹⁰⁴ The Dutch Digital Strategy, Op. Cit, p. 14. Ver Anexo 5.

¹⁰⁵ European Innovation Council — **The European Capital of Innovation Award** [Em linha]. Bruxelas: European Innovation Council, 2022.

¹⁰⁶ European Commission — **Reflection Paper: Towards a Sustainable Europe by 2030** [Em linha]. Bruxelas: European Commission, 2019, p. 19.

¹⁰⁷ KUYPER, Tijn — **City Highlight: Amsterdam** [Em Linha]. *In Medium*, 2019.

É neste sentido que o setor automóvel está, mais uma vez, no topo das estratégias implementadas. Certamente que a diminuição de tráfego e a procura de estacionamento estão na mira de estudos e uma prioridade no investimento tecnológico, porque, de facto, consomem uma grande porção das estratégias adotadas na implementação de cidades inteligentes. Uma das empresas líderes neste setor é *Too Gethr*¹⁰⁸, uma empresa que recolhe e analisa informação relativa a parques de estacionamento com o intuito de facilitar a logística da população, sendo possível a reserva de estacionamento e até a visualização em tempo real da afluência em cada momento através do uso de sistemas de Inteligência Artificial. Além disso, a empresa *Too Gethr* fornece também um serviço de recolha de transporte de passageiros mediante a sua localização e o seu horário laboral. Muito embora esta possa ser uma vantagem aparente na rotina da população, a verdade é que este é um sistema que requer informações como o horário laboral e a localização da pessoa que pretender usufruir deste serviço. Apesar de ser um serviço opcional e do seu utilizador ser previamente informado das condições do serviço, a tendência é, cada vez mais, para que todo o tipo de serviços requeira a análise de informações pessoais que revelem este tipo de informação.

Já o *City Innovation Exchange Lab*, uma empresa que trabalha com várias cidades no sentido de criar protótipos, testar e partilhar soluções inovadoras e com impacto social, tem vindo a trabalhar simultaneamente com diversas cidades com o objetivo de analisar as atividades dos cidadãos e poder estudar as suas necessidades e comportamentos. Atualmente, este laboratório tem diversos projetos em curso, sendo um deles relacionado com câmaras de vigilância, que medem as reações das pessoas quando lhes são colocadas questões controversas em relação à privacidade. Estas câmaras estão em funcionamento apenas e durante um festival *We Make the City*, um festival que tem como principal objetivo tornar as cidades melhores, abordando desafios urgentes do quotidiano tanto com o público como com especialistas, em diferentes zonas da área metropolitana de Amesterdão. No entanto, a implementação destas câmaras, ainda que apenas durante este festival, representa uma semente dos projetos já lançados e será um caminho a seguir para a realidade do futuro¹⁰⁹. Apesar disso, Amesterdão foca-se bastante em colmatar estes avanços tecnológicos com políticas de segurança e privacidade para que a cidade se consiga manter atrativa a turistas e

¹⁰⁸ Too Gethr — **Simplify Parking** [Em linha]. In Too Gethr, sd.

¹⁰⁹ City Innovation Experiment Lab — **Camara Vision Experiment** [Em Linha]. Amesterdão, 2022.

estrangeiros. Para isso, a capital holandesa tem algumas regras estabelecidas para que ninguém seja filmado ou apanhado por sensores sem o seu consentimento. Até à data, a solução encontrada passa pela colocação de avisos visíveis em todas as áreas abrangidas por estas câmaras e sensores¹¹⁰.

No entanto, vale a pena referir uma situação mais particular. Dries Depoorter, um artista digital belga, tem focado grande parte do seu trabalho na Inteligência Artificial e, inclusive, já fez experiências em que reúne dados privados detetados por câmaras abertas de várias cidades com o objetivo de alertar para a facilidade de acesso a informação privada detetável a partir destas mesmas câmaras. Esta experiência tem por base o reconhecimento facial a partir de uma fotografia do Instagram por exemplo, e, reconhecendo a pessoa, consegue detetá-la em qualquer câmara aberta no mundo e Depoorter já conseguir, efetivamente, detetar algumas pessoas em câmaras em Amesterdão através de fotografias, o que coloca em evidência uma falha que põe em causa todas as políticas de segurança implementadas por Amesterdão até ao momento e que evidencia estas mesmas falhas de segurança no domínio da privacidade dos seus cidadãos¹¹¹.

Muito embora seja crucial a colocação de avisos, e Amesterdão assegura-se da sua afixação, é também muito importante que haja infra-estruturas de segurança suficientemente desenvolvidas e testadas para que, mesmo com consentimento, não haja *leaks* de informação que possam colocar em causa a integridade da privacidade dos cidadãos. Atualmente, este tipo de infra-estruturas têm um forte impacto a nível internacional, uma vez que, sendo Amesterdão uma cidade dinâmica e com muitos projetos com empresas estrangeiras, está em causa informação que pode colocar em risco empresas de outros países. A globalidade e a conectividade têm um grande valor nas relações internacionais e, principalmente, quando envolvem empresas de vários países, são uma causa/consequência daquilo que significa ser uma cidade inteligente.

Ainda no caso de Amesterdão, há neste momento uma grande aposta no desenvolvimento das infra-estruturas, bem um foco na formação e no recrutamento de analistas de cibersegurança peritos na proteção da informação guardada no ciberespaço. Além disso, segundo Rachel Tinkamp, as imagens recolhidas por câmaras públicas não são

¹¹⁰ Privacy City of Amsterdam — **Cameras, Sensors and your privacy** [Em Linha]. In Amsterdam, sd.

¹¹¹ Sem Autor — **Back End - Dries Depoorter** [Em linha].

guardadas, mas sim imediatamente redirecionadas e apenas são guardadas as coordenadas e o número da pessoa, mas nunca informações sobre a própria pessoa¹¹². Ou seja, o que acontece é que as câmaras veem as pessoas enquanto números e não enquanto indivíduos com informações pessoais, não correndo assim o risco de invadir a privacidade de ninguém. A informação que importa recolher são comportamentos e padrões que ajudem não só a recolher dados sobre as necessidades da sociedade, mas também para a proteger. Neste sentido, e não ficando nenhuma informação pessoal armazenada, o risco de haver uma fuga de informação reduz-se a quase inexistente.

Por outro lado, a informação não é recolhida apenas pelo Estado, mas também por entidades externas/privadas que operam com o mesmo objetivo, e que por consequência contribuem para a aposta na inovação das tecnologias utilizadas.

Neste sentido, existem dois tipos de estratégias de armazenamento de informação pessoal que podem ser adotadas: a centralizada e a descentralizada. Se a primeira procura concentrar num só sítio todo o tipo de informação, a segunda procura manter diferentes tipos de informação em diferentes espaços, ficando assim minimizado o risco de apoderamento de toda a informação contida num só sítio. Já o armazenamento deste tipo de informação de forma centralizada representa um risco à privacidade se não forem adotadas medidas regulamentares que intercedam diretamente na proteção de dados. Estas medidas passam por procedimentos e políticas de auditoria que visam a proteção da informação na infraestrutura destas empresas.

Estas estratégias de segurança são cada vez mais importantes e colocam a cidade num patamar muito elevado a nível internacional. Efetivamente, o facto de uma cidade crescer digitalmente leva a que seja uma cidade global e com relações internacionais bem estabelecidas. Neste sentido, ser uma cidade segura na proteção de dados é muito importante também para o seu desenvolvimento, muito embora se mantenha o constante dilema entre desenvolvimento e proteção. Atualmente, para que possa ser desenvolvida uma tecnologia que responda às necessidades dos cidadãos, é necessário que seja recolhida e analisada a informação relativa a estas mesmas necessidades, traçando-se assim uma linha muito ténue entre o que é mais importante: conforto ou segurança?

¹¹² HACKETT, Paul — **Following the crowd: Amsterdam's smart city solution** [Em linha]. In EuroNews, 2021.

Na Estratégia Digital Holandesa 2021 um dos tópicos abordados diz precisamente respeito à salvaguarda dos direitos humanos e dos valores públicos¹¹³. Segundo esta plano, os riscos que a Inteligência Artificial apresenta são alvo de grande atenção e atuação por parte do Estado, e sendo um tópico de discussão dentro da própria sociedade, reconhecem a robustez dos quadros jurídicos no que diz respeito à proteção de dados digitais. Além de mais garantias legais, o Governo holandês reconhece ainda que se deve garantir que a lei proteja de forma clara os direitos dos cidadãos no espaço virtual — “The government notes that further clarity is required in legal practice as to how the law should be interpreted and whether sector specific interventions are necessary”¹¹⁴. Neste sentido, os Países Baixos têm vindo a contribuir de forma ativa para as discussões que decorrem no âmbito da Comissão Europeia sobre o quadro jurídico dos direitos. Tendo em conta que o tráfego de dados não conhece barreiras, é natural que uma jurisdição internacional e a cooperação entre vários países seja essencial e, pertencendo os Países Baixos à União Europeia, Amesterdão esforça-se por colaborar com a Comissão Europeia neste sentido. Na verdade, os Países Baixos têm compactuado e trabalhado bastante com as instituições europeias com o objetivo de melhorar as propostas relativas à sensibilidade de proteção de dados pessoais no ciberespaço, sendo também um país bastante crítico e com uma forte voz naquelas que são as leis da União Europeia já conhecidas em relação a este assunto, nomeadamente o Data Governance Act¹¹⁵ à qual os holandeses apontam bastantes falhas — “In November 2020, the European Commission published the Data Governance Act. This legislation aims to improve the availability of data in the EU by increasing public data sharing, by bolstering trust in data intermediaries, and by strengthening data sharing mechanisms in the EU. The Netherlands is cautiously positive, while recognising that this proposal fails to address a number of issues such as access to data”¹¹⁶.

Assim sendo, tanto a União Europeia como Amesterdão sublinham a importância da proteção de dados e a importância e urgência que existe para que todos os países membros

¹¹³ The Dutch Digital Strategy, Op. Cit, p. 14.

¹¹⁴ Idem.

¹¹⁵ Register of Commission Documents — **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)** [Em linha]. Bruxelas: Comissão Europeia, 2020.

¹¹⁶ The Dutch Digital Strategy, Op Cit, p. 18.

evoluam de forma análoga. De facto, estando perante um espaço digital, consequentemente mais difícil de controlar pela sua dimensão, para que funcione de forma coesa toda a União Europeia deve estar no mesmo nível de desenvolvimento tecnológico, principalmente no que diz respeito à maturação das infra-estruturas de segurança digital. Este é um fator importante não só para que os cidadãos europeus tenham acessos semelhantes, mas também para que cada cidadão esteja tão seguro no seu país como em qualquer outro país da União Europeia. De facto, os Países Baixos preocupam-se não só com desenvolvimento no plano regional, mas direccionam também grande parte dos seus recursos naquilo que é o desenvolvimento do plano nacional, do plano europeu e do plano internacional, tendo em curso medidas que visam a inovação e integração em todos estes domínios. A título de exemplo, em termos regionais, a estratégica holandesa passa pelo desenvolvimento da inovação industrial e da economia digital. Relativamente ao desenvolvimento nacional, procura investir no sistema digital holandês, reforçar áreas como a cibersegurança e apertar as relações com o plano digital europeu, onde procura, no plano europeu, desenvolver e acelerar a fase transitória para o digital e cooperar com a legislação a longo prazo estabelecidas pela União Europeia. Por último, no quadro internacional, os Países Baixos pretendem abrir-se ao exterior através de parcerias desde o âmbito governamental ao comercial mantendo, deste modo, a cooperação digital entre países¹¹⁷. Além disso, tendo em conta o peso e a relação direta que o desenvolvimento digital tem com a economia, é importante que este seja um trabalho conjunto entre todos os países para que a economia europeia seja mais forte e mantenha um crescimento positivo.

Neste momento, Amesterdão preocupa-se com o número de empresas que, não sendo holandesas ou europeias, têm a capacidade de determinar as regras do mundo digital e está empenhado em conseguir tornar-se mais sustentável através do recurso à tecnologia, entregando esta tarefa a empresas privadas ou semi-privadas¹¹⁸.

Neste sentido, Amesterdão tem uma política de proteção de dados bastante rigorosa. O *General Data Protection Regulation (GDPR)* garante aos cidadãos os seus direitos relativamente aos seus dados pessoais, uma legislação revista e aprovada pela Comissão Europeia em 2020. Criado em 2018, o *GDPR* é regulamentado pela União Europeia e garante

¹¹⁷ Idem, p. 47. Ver anexo 6.

¹¹⁸ Ibidem, p. 50.

a aplicação do direito de proteção de dados, aplicado a todos os cidadãos dos Estados-Membros da União Europeia e do Espaço Económico Europeu. Além de proporcionar proteção dentro do espaço europeu, é também regulamentada a exportação de dados pessoais para fora do Espaço Económico Europeu.

Amesterdão baseia-se nesta legislação para assegurar a proteção de dados aos seus cidadãos, nunca descurando a importância de a manter atualizada. Com a constante evolução tecnológica é importante haver um acompanhamento e atualização desta legislação — “The government is working on an amendment to the General Data Protection Regulation (Implementation) Act (UAVG)¹¹⁹ to provide greater clarity on the conditions for the use of biometrics for personal identification”¹²⁰.

O trabalho que Amesterdão tem vindo a desenvolver no âmbito da tecnologia e da Inteligência Artificial tem, na verdade, colocado esta cidade numa posição internacional bastante relevante para o desenvolvimento do país. Segundo os dados mais recentes da análise europeia de 2022 feita pelo Índice de Digitalidade da Economia e da Sociedade (*DESI*), os Países Baixos ocupam o terceiro lugar na escala europeia, o que muito se deve ao desenvolvimento de Amesterdão. Este índice acompanha o desenvolvimento digital dos Estados-Membros e analisa os esforços feitos por cada Estado-Membro para colmatar lacunas no domínio digital¹²¹. Entram em análise, por exemplo, o capital humano, a conectividade, a integração da tecnologia digital e a digitalização de serviços públicos. Segundo este relatório, os Países Baixos estão no pódio em todos os setores¹²², impulsionando assim a importância do desenvolvimento tecnológico de Amesterdão no quadro das relações internacionais.

Tendo em conta o carácter global das cidades inteligentes, é também importante analisar o que tem acontecido noutros espaços fora da Europa. Não obstante o desenvolvimento positivo a que se tem assistido na última década, é relevante perceber quão envolvido está o espaço europeu no desenvolvimento tecnológico comparativamente a países externos à Europa. Olhando para o espaço asiático, a 1 de abril de 2017 a China anunciou a decisão de, na província de Hebei, criar um projeto de escala nacional de alta qualidade com

¹¹⁹ *Ato de Implementação do Regulamento Geral de Proteção de Dados*, na sigla holandesa.

¹²⁰ The Dutch Digital Strategy, Op. cit, pp. 18-19.

¹²¹ Comissão Europeia — **Índice de Economia e Sociedade Digitais (DESI)** [Em linha]. Bruxelas: Comissão Europeia, sd.

¹²² Ver anexo 7.

foco num sistema económico moderno. Esta decisão recaiu sobre a criação de raiz de uma cidade com altas competências tecnológicas e de confiança, para onde pudessem ser migrados projetos de Pequim, de modo a aliviar a capital chinesa. Por este motivo, a localização da cidade Xiong'an New Area releva-se estratégica e localiza-se perto da capital chinesa, tal como é representada no seguinte mapa.

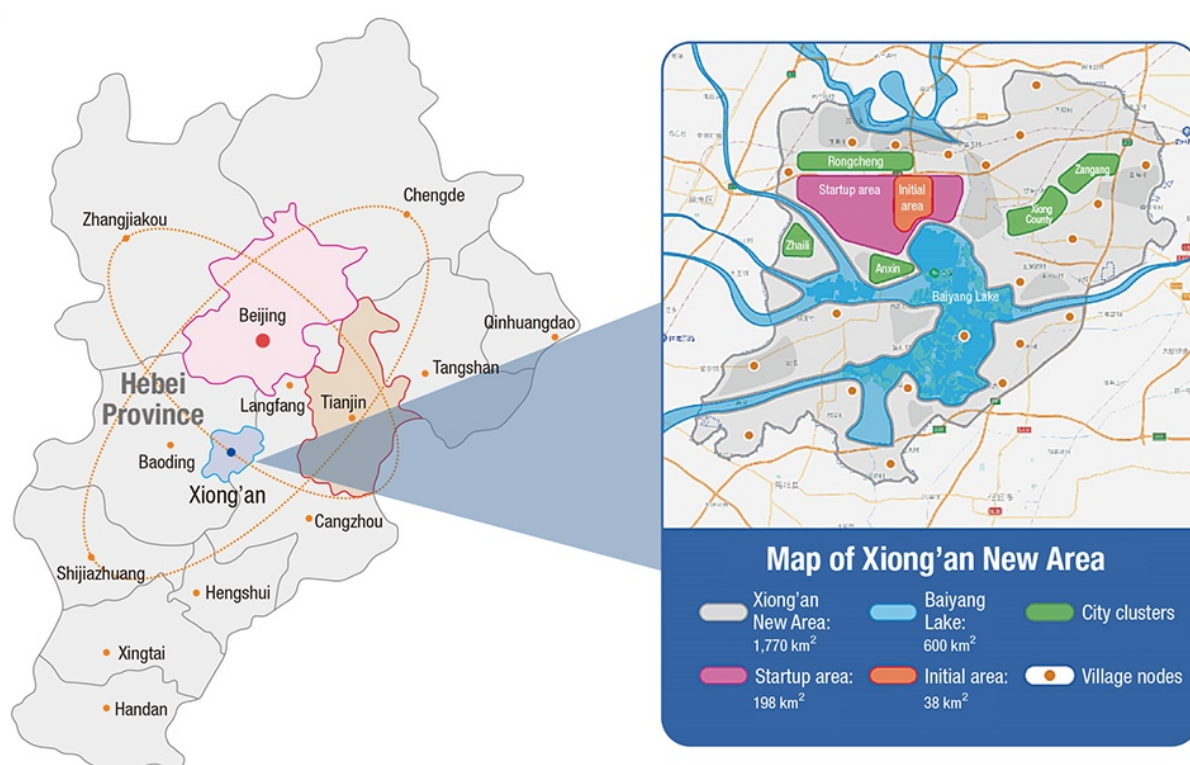


Figura 1: Mapa da nova zona de Xiong'an e panorâmica do desenvolvimento¹²³.

De facto, Xiong'an New Area é uma cidade do futuro, uma vez que foi criada e está a ser desenvolvida com tecnologia de ponta e visa oferecer aos seus habitantes conforto e bem-estar através da Inteligência Artificial. Segundo um artigo de Chen Yangqiu, Lai Ning e Zhang Xueting (2021), apesar desta cidade ter sido criada em 2017 foi na era pós-COVID que teve

¹²³ YANGQIU, Chen; NING, Lai; XUETING, Zhang — China's City of the Future: Xiong'an New Area. *Innovations to Improve People's Quality of Life* [Em linha]. 70:1 (2021).

um grande impulso no seu desenvolvimento, reforçando a sua aposta na Inteligência Artificial enquanto motor da gestão e desenvolvimento da cidade em diversas áreas — “There will be an increased emphasis on quality of life (QoL) considerations such as health, safety, and livability achieved through smarter urban construction, with government investment in new infrastructure strengthening such areas as 5th-generation (5G) telecommunications, artificial intelligence (AI), and data centers”¹²⁴. Após o início da construção da cidade, a 7 de dezembro de 2017, demorou apenas 117 dias para que a obra estivesse concluída, num área total de 99,600 metros quadrados e com a área de serviço público, de serviço administrativo, de serviço de estilo de vida e de escritórios de uma empresa completamente funcionais¹²⁵. Claramente que esta capacidade chinesa vai muito além daquilo que hoje é possível fazer na Europa.

Para 2035, os propósitos da liderança chinesa para esta cidade-modelo estão direcionados para a inteligência inovadora, para a tecnologia verde e para o bem-estar populacional, sendo que o principal objetivo é o alcance da liderança tecnológica e científica a nível internacional, mantendo sempre firme a segurança.

Neste sentido, o governo chinês tem vindo a apostar na última década na construção de cidades mais ecológicas e mais inteligentes, capazes de oferecer melhor qualidade de vida. Por isso, a criação deste tipo de cidades-modelo são uma aposta chinesa que visa incentivar a qualidade de vida nas cidades. Esta capacidade reflete-se no poder e influência económica chinesa, na sua mentalidade de progresso e no foco dos avanços a longo prazo, procurando não só criar novas cidades, como também atualizar as cidades já existentes.

Apesar disso, importa notar que a segurança, por ser um objetivo de Xi Jinping, tem sido reforçada a um ponto que pode colocar em causa a privacidade e liberdade da população chinesa, isto porque as cidades chinesas dispõem de uma forte vigilância e monitorização detalhada de todos os passos das pessoas. A título de exemplo, existe em média um *CCTV*¹²⁶ para cada duas pessoas e estas são câmaras que utilizam o reconhecimento facial e a tecnologia de deteção de emoções para, assim, conseguirem prever comportamentos

¹²⁴ Idem.

¹²⁵ Ibidem.

¹²⁶ *Circuito Fechado de Televisão*, na sigla inglesa.

problemáticos¹²⁷. Neste sentido, importa refletir sobre o facto do exponencial avanço tecnológico chinês estar a condenar a privacidade da população chinesa e sobre qual o impacto que isso poderá ter na Europa. Dependerá a segurança da violação dos direitos de privacidade? Será que para ser possível acompanhar o progresso chinês teremos de prescindir da nossa privacidade? As respostas a estas perguntas não são inequívocas, mas a verdade é que existe uma relação entre ambas e não podemos desvalorizar o equilíbrio entre qualidade de vida e privacidade. Embora as cidades-modelo chinesas continuem a evoluir e a crescer em número, a Europa continua a tentar manter a sua posição e é essencial manter uma coesão tecnológica entre os países europeus.

Por isso, Amesterdão acolhe um grande leque de empresas de tecnologia digital e inovação, principalmente no que diz respeito à Inteligência Artificial. Esta é uma causa/consequência muito relevante no âmbito das relações internacionais, uma vez que Amesterdão acolhe muitas empresas estrangeiras que optam por se sediar nesta cidade pela capacidade de desenvolvimento e oferta de oportunidades. Empresas como a *Dutch Artificial Intelligence Coalition*, a *Dutch Blockchain Coalition* e a *Smart Industry Program* procuram o impulso na capital holandesa, o que também acaba por reconhecer internacionalmente a importância do desenvolvimento tecnológico de Amesterdão.

Para a Comissão Europeia, este cenário é bastante positivo, já que incentivar o crescimento de cidades inteligentes é um objetivo destacado na sua agenda para 2030, porque lhes permite alavancar o destaque europeu no quadro mundial. A Comissão Europeia apresentou já várias propostas ao Conselho Europeu visando impulsionar o crescimento de uma Europa Digital, desde reformas políticas a soluções ecológicas. Na realidade, este tem sido um assunto recorrentemente debatido no Parlamento Europeu, onde estão neste momento em curso debates não só sobre as regras para um ambiente digital seguro e competitivo, mas também sobre a política dos consumidores para as transições ecológica e digital¹²⁸.

No que diz respeito às regras para um ambiente digital seguro e competitivo, existem vários assuntos a serem debatidos no Parlamento Europeu. Primeiramente, o reforço da importância dos princípios éticos e a necessidade de promover a igualdade de género, bem como proteger os consumidores e manter a *internet* um espaço neutro, fidedigno e inclusivo.

¹²⁷ FAN, Wu — **Smart Cities Deep Dive: AI-Powered Urbanization** [Em linha]. In China Talk, 2023.

¹²⁸ Parlamento Europeu — **Prioridades e contributos do Parlamento Europeu** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2023.

Depois, e como a Inteligência Artificial tem sido, e é já, uma presença constante, a 14 de junho de 2023 houve no Parlamento Europeu uma sessão plenária com o intuito de discutir e negociar as primeiras regras para a inteligência artificial¹²⁹, entre as quais:

- **Proibição de sistemas de identificação biométrica à distância em tempo real**¹³⁰.

Este é um sistema de autenticação que deteta características específicas de cada pessoa, por exemplo, impressões digitais, padrões faciais, voz, ADN e até mesmo medição das mãos e da íris. Este dispositivo mede e recolhe estes dados que são, posteriormente, armazenados num sistema de *software*¹³¹. Este sistema já é bastante usado nos smartphones, onde o utilizador fornece a impressão digital ou o reconhecimento facial para que depois consiga aceder facilmente ao dispositivo através do reconhecimento do sistema dos dados que forneceu. Segundo o Parlamento Europeu, este sistema é proibido quando utilizado à distância, nomeadamente com o fim de fazer um reconhecimento de emoções, ao contrário do que acontece na China, como referido anteriormente. Salvo para repressão criminal, esta lei aplica-se a todos os sistemas que, através de câmaras de vigilância, consigam detetar os dados pessoais de um indivíduo através do reconhecimento facial, como por exemplo: idade, género, etnia, identificação fiscal, orientação política, etc.¹³².

- **Proibição de Inteligência Artificial generativa** (exemplo: *CHatGPT*) sem a nota prévia de que a informação presente foi gerada pela IA¹³³. Com a facilidade com que se obtém qualquer tipo de informação, imagens, vídeos e áudios, criados através de plataformas com sistema de IA generativa, é crucial que seja claro que a informação provém da sua utilização, para que seja mais fácil distinguir e analisar possíveis manipulações de imagens e vídeos. Embora o *ChatGPT*, por exemplo, possa servir

¹²⁹ Parlamento Europeu — **Parlamento negocia primeiras regras para inteligência artificial mais segura** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2023.

¹³⁰ Idem.

¹³¹ Sem Autor — **Identificação e dados biométricos, sabe o que são?** [Em linha]. In Notas em Dia, 2023.

¹³² Anexo 6.

¹³³ Parlamento Europeu — **Parlamento negocia primeiras regras para inteligência artificial mais segura**, Op. cit.

como uma ferramenta útil de trabalho, é importante ter em atenção que a manipulação de informação é um risco e, que por isso, é crucial que haja um controlo sobre a sua utilização.

- **Proibição de sistemas de IA para influenciar eleitores nas campanhas eleitorais**¹³⁴. Esta lei visa combater o recurso à IA para influenciar e manipular as crenças e pensamentos humanos. Com a quantidade de dados recolhidos sobre cada pessoa (por exemplo através dos já referidos sistemas biométricos) é fundamental haver um controlo minucioso sobre o uso desta informação. Como já foi analisado previamente, a utilização das redes sociais pode tornar-se uma desvantagem quando direcionada para a influenciar as convicções das pessoas e, assim, redirecionar as suas opções políticas. O direito ao livre arbítrio não deve ser posto em causa, principalmente quando são utilizados dados pessoais para manipular os ideais dos próprios indivíduos.

Já em relação à política dos consumidores para as transições ecológica e digital discutida no Parlamento Europeu, foi acordado entre os eurodeputados que é importante regular os mercados e serviços digitais, além de ser necessário tornar o mercado digital circular e sustentável — por exemplo, através da reciclagem de baterias e de sistemas de reparação que evitem o desperdício tecnológico.

Relativamente à nova regulamentação sobre mercados e serviços digitais, foram compiladas medidas para combater conteúdos digitais ilegais ao mesmo tempo que se respeita a liberdade de expressão e a proteção de dados pessoais; o controlo mais apertado aos comerciantes digitais; controlo dos algoritmos para que haja uma maior transparências das plataformas; e também a proibição de publicidades com o intuito de manipular a decisão do consumidor¹³⁵. Estas regras foram definidas já em 2022 e continuam a ser discutidas e melhoradas no Parlamento Europeu, nomeadamente com a discussão do *Digital Services Act*, do Regulamento da Proteção de Dados e da Inteligência Artificial, bem como do *Data Act*. A nível da Regulamentação da Inteligência Artificial, incluindo o uso das câmaras biométricas,

¹³⁴ Idem.

¹³⁵ Parlamento Europeu — **Serviços digitais: novas regras para um ambiente em linha mais seguro e aberto** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2022.

falta ainda esclarecer a posição da Comissão Europeia relativamente a este tema e negociar a permissão, ou recusa, do uso efetivo dos dados biométricos.

Para assegurar e reforçar a segurança dos cidadãos europeus, o Conselho Europeu assinou, em conjunto com a NATO, a 10 de janeiro de 2023, uma declaração com vista a alargar a cooperação entre ambas as entidades. Esta declaração promove diversas estratégias de paz, naturalmente atenta à guerra da Rússia contra a Ucrânia, mas também alarga estas relações através do reforço da proteção de infraestruturas críticas e das tecnologias emergentes disruptivas. Além disso, aprofundam a identificação e o combate à manipulação de informação por parte de agentes estrangeiros, nomeadamente com recurso a tecnologia generativa¹³⁶.

Neste contexto não podem, pois, ficar de parte regulamentos que preservem a segurança digital, como o Regulamento Governação de Dados, o Regulamento Serviços Digitais, o Regulamento Mercados Digitais e a Estratégia de Cibersegurança¹³⁷. Pelo peso que a transição para a digitalização tem para a Europa, todos estes processos são financiados pela União Europeia, nomeadamente no que diz respeito à formação e educação dos cidadãos, dado que o conhecimento básico do digital, aliado à contratação de especialistas na área, são a melhor forma de prevenir e ajudar a combater o cibercrime.

Neste sentido, em março de 2021 a Comissão Europeia apresentou quatro objetivos fundamentais para tornar a Europa mais digital¹³⁸ de uma maneira mais segura, sendo elas:

- **Investir na formação da população e de profissionais do setor digital.** Este objetivo foca-se, principalmente, em dotar os cidadãos do conhecimento digital necessário para que possam dominar este espaço. Sendo que é uma realidade inevitável e um objetivo europeu, é importante que os cidadãos sejam capazes de acompanhar todo o processo. Por isso mesmo, a Comissão Europeia considera as competências básicas como um direito dos cidadãos. Para colmatar este objetivo, a Comissão propõe, até 2030, “Para além da meta em matéria de competências

¹³⁶ Conselho Europeu — **Declaração Conjunta sobre a cooperação UE-OTAN, 10 de janeiro de 2023** [Em linha]. Bruxelas: Conselho Europeu, 2023.

¹³⁷ Comissão Europeia — **Orientações para a Digitalização até 2030: a via europeia para a Década Digital** [Em linha]. Bruxelas: Comissão Europeia, 2021.

¹³⁸ Idem.

digitais básicas estabelecida no Plano de Ação sobre o Pilar Europeu dos Direitos Sociais, a existência de 20 milhões de especialistas em TIC empregados na UE, com uma preocupação de paridade entre homens e mulheres”¹³⁹.

- **Tornar mais seguras e eficazes as infra-estruturas digitais.** Efetivamente, para que possam ser implementadas novas tecnologias, é essencial que haja infra-estruturas de redes fixas e móveis capazes e com potencial para a execução de tarefas rápidas e eficazes, bem como com espaço para o futuro desenvolvimento da rede móvel 6G. Por isso, neste ponto, o compromisso da Comissão Europeia é proporcionar “A cobertura de todos os agregados familiares europeus por uma rede a *gigabits*, com todas as zonas povoadas abrangidas pela 5G”¹⁴⁰. Como já foi descrito no capítulo anterior, com a chegada da computação quântica é necessário que haja um investimento de infraestruturas a longo e médio prazo. Embora a computação quântica ainda esteja numa fase de desenvolvimento, é certo que o progresso já em curso vai pôr em evidência a necessidade do desenvolvimento das infra-estruturas para que possam acompanhar e suportar o desenvolvimento tecnológico. Faz parte, portanto, dos objetivos da União Europeia ter, até 2025, o seu primeiro computador com aceleração quântica, uma vez que só assim será possível manter a Europa nesta competição tecnológica.

- **Investir na digitalização das empresas.** Consequência da situação pandémica, houve já muitas empresas que foram, de certa forma, obrigadas a recorrer ao digital. Verificando-se que a maioria delas já não quis regressar ao formato presencial anterior a 2020, pretende-se que este número aumente até 2030. A Comissão Europeia pretende também investir em diversos setores, como agricultura, saúde, mobilidade e até mesmo transformação de indústrias. Como foi já referido nesta investigação, a chegada da rede móvel 5G já proporcionou a transformação digital de muitas indústrias e hoje o termo *indústria 5G* é já uma realidade. Por isso, será inevitável que este seja um objetivo da Comissão Europeia, até porque a inovação

¹³⁹ Ibidem.

¹⁴⁰ Ibidem.

de ponta disruptiva é um fator chave para um mercado único funcional capaz de fazer concorrência com outros países com peso no mercado internacional, como os EUA e a China. Por isso, até 2030, um dos objetivos da Comissão Europeia passa por fomentar “A utilização de serviços de computação em nuvem, megadados e inteligência artificial por 75 % das empresas europeias”¹⁴¹.

- **Investir na digitalização de serviços públicos.** Por último, neste objetivo, existe o compromisso por parte da Comissão Europeia de, entre outros aspetos, promover “A disponibilização aos cidadãos e às empresas europeias da prestação de serviços públicos essenciais 100 % por via eletrónica”¹⁴². Aliado à Inteligência Artificial, pretende-se que o Governo implemente a digitalização de serviços públicos, como a telemedicina, o voto digital e até mesmo formas de identificação digital. Em Portugal já existe uma *app* administrada pelo Governo onde são guardados os documentos de identificação, como o cartão de cidadão e a carta de condução, que são plenamente válidos e que podem substituir a versão física. É, por isso, um objetivo tornar os serviços públicos mais práticos e de mais fácil acesso.

Comparando os objetivos da Comissão Europeia com o crescimento e desenvolvimento digital de Amesterdão, podemos concluir que a capital holandesa tem sido uma referência positiva para a concretização dos objetivos europeus, não só através da implementação da Inteligência Artificial, mas também com o desenvolvimento digital das empresas, que ao mesmo tempo promovem a Economia 5G e o mercado único.

É ainda relevante perceber como é que os EUA estão comparativamente à Europa e à China, de modo a ter um fator de comparação e melhor entender a postura de Amesterdão face a outras potências promissoras. Veja-se, por exemplo o caso da cidade de Nova Iorque (*NYC*). A organização sem fins lucrativos, *NYCEDC*¹⁴³, tem vindo a apostar no desenvolvimento económico e tecnológico de Nova Iorque a fim de tornar esta cidade mais apelativa para a criação de negócios e ao mesmo tempo mais inteligente, sustentável e resiliente. Deste modo,

¹⁴¹ Ibidem.

¹⁴² Ibidem.

¹⁴³ *A New York City Economic Development Corporation*, na sigla inglesa.

esta entidade trabalha muito no sentido da sustentabilidade e do combate às alterações climáticas, acreditando que só assim, as empresas terão um lugar adequado para desenvolver os seus negócios e utilizar os recursos da cidade a seu favor — “It’s our mission to ensure that companies have the space and resources they need to source and train talent, conduct and amplify research, connect investors to entrepreneurs, pilot new technologies, and demonstrate solutions”¹⁴⁴. Por isso, os empresários e as empresas de tecnologia são apoiadas por esta entidade a fim de apostarem no desenvolvimento tecnológico da cidade nova iorquina, ao mesmo tempo que asseguram que este desenvolvimento chega à população para, assim, melhorar a sua qualidade de vida.

A verdade é que *NYC* incentiva e acolhe empresas tecnológicas, porque todo o plano estratégico de desenvolvimento da cidade visa a transformação de *NYC* numa cidade inteligente cada vez mais forte e bem equipada em todas as áreas: na medicina, na aplicação da lei, na educação, na mobilidade, na ciência, etc. A título de exemplo, a empresa Hellman Electric, uma empresa norte americana que começou por ser de construção pesada e se tornou numa empresa de construção elétrica, definiu recentemente objetivos muito claros quanto ao progresso de *NYC* enquanto cidade inteligente e quanto ao modo como a tecnologia está, inevitavelmente, associada ao bem-estar da população. No âmbito da segurança, a deteção inteligentes de ameaças acelera o tempo de resposta, pelo que a polícia de *NYC* criou uma parceria com a empresa *Microsoft* para desenvolverem o *Domain Awareness System*, isto é, um programa que mede e deteta crimes e que tem sido bem sucedida. Como resultado desse espaço tem havido uma redução do nível de criminalidade¹⁴⁵ e não falamos só da criminalidade digital. Efetivamente, segundo um relatório da *NYPD*¹⁴⁶ a percentagem de crimes tem vindo a diminuir e, comparativamente a junho de 2022, o mês de junho de 2023 viu o número de crimes diminuir consideravelmente¹⁴⁷.

Pode assim verificar-se que *NYC* tem vindo a aplicar a IA na própria segurança da cidade e que tem tido sucesso, ao ponto de já comercializar este tipo de serviço para outras

¹⁴⁴ Sem autor — **Smart Cities Supporting tech-enabled urban development to solve the most pressing challenges facing NYC and the world** [Em linha]. In NYCEDC, s.d.

¹⁴⁵ Hellman Electric — **Big Apple, Smart City. How New York Is Fast Becoming the Greatest Smart City in the World** [Em linha]. In Hellman Electric, 2019, p. 3.

¹⁴⁶ *New York Police Department*, na sigla inglesa.

¹⁴⁷ NYPD — **NYPD Announces Citywide Crime Statistics for June 2023** [Em linha]. In NYPD Media Report, 2023.

cidades. Mas, não é só nesta área que se podem ver avanços tecnológicos. Podem também ser referidos avanços na gestão do tráfego, nos contadores de água inteligentes, na gestão inteligente do lixo e até na iluminação inteligente. Estes são alguns aspetos que têm vindo a ser aplicados na gestão da cidade nove iorquina e cuja aplicação tem tido bastante sucesso. A nível do tráfego, o objetivo é que, já em 2025 o congestionamento de trânsito tenha diminuído e que a tecnologia inteligente tenha poupado, em média, 15 minutos de viagem, o que impacta positivamente também o ambiente e a emissão de gases. O programa *Midtown in Motion* tem como principal objetivo gerir o tráfego da cidade através de sensores, imagens em tempo real e recolha de dados dos veículos congestionados para, assim, operar de modo a prevenir o aumento deste congestionamento. Na verdade, a primeira vez que este programa foi implementado foi em 2012, mas mais recentemente, tem vindo a investir-se mais na aplicação da IA nesta ação.

Seguindo esta ordem de ideias, a poupança de energia é também fundamental para a sustentabilidade da cidade e tem um valor estimado de 800.000 USD poupados anualmente¹⁴⁸. Isto é possível não só pela utilização de luzes *LED*, que só por si já consomem menos, mas também pela aplicação de sensores nas luminárias, o que permite que não se esteja constantemente a consumir a mesma quantidade de luz, mas sim que isso seja regulada pela necessidade, isto é, reduz ou desliga quando não há movimento e aumenta a intensidade quando passam pessoas ou carros. A verdade é que esta pequena mudança tem um grande impacto na poupança de energia e na sustentabilidade da cidade.

Relativamente à gestão do consumo de água, estão a ser implementados contadores inteligentes que monitorizam os consumos feitos pelos seus clientes e lhes envia essa informação para que estejam mais conscientes da quantidade de água que estão a consumir. Isto pode ser controlado através de uma *app* que está ligada ao contador e que em tempo real fornece toda a informação necessária¹⁴⁹.

Por último, no que diz respeito à gestão de resíduos, a cidade está a ser dotada de contentores inteligentes que permite fazer uma melhor gestão do lixo. Estes contentores estão equipados com sensores que informam as entidades recoletoras de lixo quando estão cheio e, automaticamente, é gerado um circuito com os contentores que devem ser recolhidos por

¹⁴⁸ TOBIAS, Michael — **How New York is Becoming a Smart City** [Em linha]. In Nearby Engineers, s.d.

¹⁴⁹ Hellman Electric, Op. cit, p. 9.

ordem de urgência. Este sistema é bastante vantajoso, na medida em que poupa recursos e reduz, naturalmente, a emissão de CO2 durante todo este processo¹⁵⁰.

Comparativamente a Nova Iorque, Amesterdão também já promove todas estas iniciativas e, inclusive, ganhou um prémio Europol de excelência na inovação. Este prémio foi atribuído por um painel composto pela Comissão Europeia para os assuntos internos, chefes de polícia de Espanha, Bélgica e Hungria e pela diretora executiva da Europol¹⁵¹. Além deste prémio, Amesterdão ganhou também o prémio na categoria da iniciativa inovadora no domínio da ética, da diversidade e da inclusão.

Os Países Baixos ficaram merecedores deste prémio pela utilização da realidade virtual por parte dos agentes da polícia holandesa para criarem simulações e cenários do mundo real que podem suar preconceitos negativos, permitindo que haja, *à posteriori*, uma ação mais eficaz e preventiva por parte da polícia holandesa.

Amesterdão é, de facto, uma cidade bastante desenvolvida tecnologicamente e muito reconhecida a nível internacional enquanto cidade inteligente. Mesmo quando comparada à grande cidade nova iorquina, a capital holandesa usufrui já de bastantes equipamentos inteligentes, que promovem não só a qualidade de vida da população, mas também a sua segurança. Além disso, comparativamente à cidade chinesa Xiong'an New Area, Amesterdão, também por fazer parte da União Europeia, segue medidas de segurança muito mais apertadas, principalmente no que diz respeito ao tipo de dados passíveis de serem recolhidos e armazenados pela IA.

¹⁵⁰ TOBIAS, Michael, Op. cit.

¹⁵¹ Europol — **Netherlands, France and Estonia win the 2023 Europol Excellence Awards in Innovation** [Em linha]. In Europol, 2023.

Capítulo 4 | Resultados das Análises Comparativas

Londres e Amesterdão são, logo à partida, duas cidades muito diferentes, tanto a nível cultural, como a nível político e económico. Em termos estatísticos a nível populacional, em 2020 Amesterdão contava com cerca de 872 mil habitantes¹⁵² enquanto Londres ultrapassava os 9 milhões de habitantes¹⁵³. Tendo em conta aquilo que tem vindo a ser discutido nesta investigação, a tecnologia e a sua aplicação tem sempre como principal objetivo o aumento da qualidade de vida dos cidadãos. Assim sendo, Londres enfrenta um maior desafio, uma vez que respeita um alvo muito maior, logo, muito mais diversificado.

Embora as estratégias de cada uma destas cidades seja diferente, como foi possível constatar no capítulo anterior, é certo que ambas se focam em objetivos muito semelhantes. Como é evidente no Plano de Londres 2021, a estratégia londrina é bastante centrada em melhorar a qualidade de vida das pessoas através do crescimento de negócios, pelo que existe um grande foco nesta área. Ou seja, é a partir do desenvolvimento das atividades económicas que se procura ter melhor condições de vida. Ao invés disso, Amesterdão trabalha no sentido de melhorar primeiro a rede de conexão das pessoas para que deste ponto possam surgir novos *startups*. Para que esta conexão seja possível e facilitada, foi criada a plataforma *Amsterdam Smart City*¹⁵⁴ onde qualquer cidadão disposto a isso se pode conectar com outros cidadãos e, assim, discutir ideias e criar negócios. Embora o Governo tenha um papel bastante ativo em ambas as cidades, a verdade é que a sua intervenção diverge mediante as estratégias predefinidas.

Neste momento, Londres foca-se bastante no setor automóvel e tem perspetivas de futuro bastante concentradas na computação quântica, como referido anteriormente, um tipo de tecnologia muito avançada, o que comprova a estratégia adotada por Londres relativamente à aposta em grandes indústrias e grandes empresas. É com este tipo de investimentos que Londres se procura colocar na vanguarda, como uma das cidades mais empenhadas nas Relações Internacionais, tendo em conta a importância deste avanço tecnológico. Já em Amesterdão, onde embora também tenha sido feito um grande investimento no setor automóvel, não prevalece nenhum tipo de ambição a este nível, mas sim num investimento

¹⁵² Statista — **Total population of Amsterdam from 2009 to 2022** [Em linha]. In Statista, sd.

¹⁵³ London Data Source — **London's Population** [Em linha]. In London Data Source, sd.

¹⁵⁴ Amsterdam Smart City — **Amsterdam Economic Board** [Em linha].

naquilo que poderá intervir diretamente com os seus cidadãos. Entre Londres e Amesterdão, nota-se uma clara diferença. Com a primeira a ansiar por uma liderança global e a segunda por uma liderança europeia. Aliás, as perspetivas de futuro de ambas as cidades comprovam estas ambições: Londres aposta em promover grandes empresas multinacionais, enquanto Amesterdão se esforça por incentivar a melhoria da qualidade de vida dos cidadãos, bem como das suas empresas, considerando sempre as estratégias que os próprios cidadãos consideram mais relevantes.

Segundo Stephen Lorimer, Diretor da *Smart London Strategy*, *Great London Authority*, Londres é uma cidade que procura aprender com outras cidades mundiais, mas com o objetivo de se manter sempre à frente da curva de desenvolvimento tecnológico e nunca se limita a acompanhá-la, o que apenas será possível concretizar através da colaboração das instituições públicas com os cidadãos londrinos — “To stay ahead of the technology curve, rather than follow it, a Smarter London needs new and effective city-wide collaboration between public institutions, utilities, our world-class creative, scientific research and tech communities by and for Londoners”¹⁵⁵. Na abordagem estabelecida por Londres pretende-se absorver das cidades inteligentes mais desenvolvidas no plano mundial a maior quantidade de informação possível para, deste modo, poder pensar em soluções de longo prazo que viabilizem o desenvolvimento da cidade. Embora a solução para os desafios colocados a curto prazo também mereça o seu espaço de análise, é para o futuro que Londres olha e é no futuro que coloca a sua atenção e as suas estratégias atuais.

Segundo Lisa Smith, para Amesterdão uma verdadeira cidade inteligente sempre se focou em quatro fatores cruciais e sem os quais não seria possível transformar Amesterdão numa das mais avançadas cidades inteligentes a nível europeu. São elas o governo, as empresas, as universidades e instituições de pesquisa e os cidadãos — “Holistic approaches modeled on a quadruple helix concept – government, businesses, universities & research institutions, and citizens – are key to the creation of a truly smart city.”¹⁵⁶. Ainda segundo esta autora, é baseado neste pensamento que Amesterdão assenta a sua abordagem *bottom-up*, isto é, uma metodologia que se preocupa no investimento nas mais diversas áreas da economia

¹⁵⁵ LORIMER, Stephan — **How our plans for Smart London compare to other world cities** [Em linha]. London: Smart London, 2018.

¹⁵⁶ SMITH, Lisa — **Amsterdam Smart City: A World Leader in Smart City Development** [Em linha]. In Bee Smart City, 2017.

para que a partir daí possam surgir ambientes, governos, mobilidade e pessoas tecnologicamente mais avançados¹⁵⁷.

Apesar destas divergências, tanto Londres como Amsterdão têm alguns objetivos em comum. Tendo em conta a importância que estas cidades têm a nível internacional e tendo em conta os assuntos prementes da atualidade, é natural que o tema *sustentabilidade* seja recorrente em ambas as abordagens. Tenham muitas diferenças ou sejam movidas pelas mesmas razões, o que é certo é que ambas as cidades se encontram atualmente muito focadas e com objetivos muito concretos em relação a este tema.

Fazendo parte da União Europeia, Amsterdão tem o grande objetivo de se focar na redução dos gases de emissão propostos pela Comissão Europeia, como referido no capítulo anterior. Neste sentido, é conveniente que parte dos investimentos tecnológicos feitos em Amsterdão estejam direcionados para o setor automóvel e, principalmente, na redução de tráfego. Os veículos elétricos e as estratégias expostas no capítulo anterior para redução de tráfego são bastante promissoras e pretendem dar resposta àquilo que é não só um objetivo holandês, mas, principalmente, um objetivo europeu. Por outro lado, o aumento de circulação de bicicletas e a redução de lixo fazem também parte deste programa, pelo que a gestão de recolha de lixo já está a ser adaptada e prevê-se que em breve não só as ruas tenham câmaras capazes de detetar a quantidade e o tipo de lixo que se encontra depositado nos pontos de recolha, mas também que os camiões de recolha sejam equipados com câmaras que possibilitem quantificar a quantidade de lixo que se encontram nas ruas¹⁵⁸.

Tal como Amsterdão, também Londres não pode fechar os olhos a este tema. Aliás, no Plano para Londres 2021 a sustentabilidade é um tema bastante recorrente, havendo uma parte desse plano inteiramente dedicado a tornar Londres mais verde, começando pelas infra-estruturas. Alguns dos maiores objetivos neste plano são, precisamente, melhorar a qualidade do ar, diminuir as emissões de gases, aumentar a quantidade de energias renováveis e mitigar o aquecimento global¹⁵⁹. Uma vez mais, para assegurar que estes objetivos são cumpridos, Londres coloca na inovação tecnológica um grande peso de responsabilidade e de contribuição.

¹⁵⁷ Idem.

¹⁵⁸ Sem autor — **Smart Cities Around the World: Amsterdam Edition** [Em linha]. In GovTech Singapore, 2021.

¹⁵⁹ Mayor Of London Op. cit.

Efetivamente, Londres e Amesterdão são, atualmente, duas grandes cidades inteligentes a nível mundial, mas principalmente a nível europeu. O seu crescimento e desenvolvimento dependem muito do estado em que cada cidade se encontra, mas também dos objetivos que tem em termos de desenvolvimento interno e de reconhecimento internacional. Tanto Londres como Amesterdão são cidades muito fortes a nível mundial, pelo que o acompanhamento do seu desenvolvimento é uma evidência do trajeto que as relações internacionais estão a tomar, principalmente no que diz respeito às suas relações e formas de demonstração de poder. No âmbito da tecnologia, as cidades referidas abrem caminho para que outras cidades apostem também no seu desenvolvimento tecnológico, uma vez que a perspectiva de progressão e crescimento são palpáveis. Por outro lado, a tecnologia originou uma corrida pelo poder que só é possível ter através da própria tecnologia e que altera o foco das relações inter-estatais. Com a revolução tecnológica, no século XXI o desenvolvimento de uma cidade neste setor dita muito do seu poder e alcance. É muito importante ter cidades como Londres e Amesterdão no quadro europeu, para que, comparativamente a outras cidades médias, como referidos anteriormente, possam cumprir com a dinâmica sentida atualmente. Claro que, embora possam divergir em diversas áreas, formas de atuação e objetivos, o crescimento tanto da cidade londrina como de Amesterdão enquanto cidades inteligentes encontra-se já num nível avançado e são hoje referências mundiais de sucesso e de modelo a seguir.

Apesar de Londres e Amesterdão serem duas cidades diferentes, como já foi possível explorar no decorrer desta investigação, ambas têm traçado caminhos importantes no avanço da tecnologia, principalmente na sua relação com a vida quotidiana. Os maiores desafios a serem enfrentados são, sem dúvida, a questão da segurança e da proteção de dados e a abertura deste caminho no âmbito da tecnologia tem um peso muito grande para as relações internacionais e para a geopolítica. A emergência de novas cidades inteligentes inspiradas noutras cidades inteligentes tem um grande significado político e desde 2020 que cerca de 50 países se têm vindo a desenvolver tecnologicamente, incluindo países da União Europeia, principalmente em áreas como a Inteligência Artificial¹⁶⁰.

¹⁶⁰ TINNIRELLO, Maurizio — The Global Politics of Artificial Intelligence. ULNICANE, Inga [*et al.*] — **Governance of Artificial Intelligence: Emerging International Trends and Policy Frames** [Em linha]. CRC Press: London, 2022, p. 38.

Perante as Relações Internacionais, ambas as cidades têm um impacto bastante evidente, na medida em que o avanço tecnológico e o recurso à Inteligência Artificial têm implicações diretas tanto em conflitos internacionais como na cooperação internacional. Neste sentido, não se pode ignorar a importância que tudo isto tem para a cooperação internacional. Primeiro, porque apesar dos desafios que a falta de barreiras físicas acarreta, principalmente em relação à segurança, é muito mais facilitada a solução de problemas globais, nomeadamente das mudanças climáticas e do controlo da poluição do ar (conduzida, maioritariamente, através de estratégias sustentáveis no controlo do tráfego urbano, por exemplo) o que levará, inevitavelmente, à redução da emissão de dióxido de carbono e da poluição sonora.

Depois, é importante também ter em conta o intercâmbio do conhecimento, uma vez que, por exemplo, a inovação tecnológica permite a partilha dos avanços e recuos, tal como podemos ver nos casos de Londres e de Amesterdão. Mas, um dos pontos mais cruciais e vantajoso é a cooperação empresarial, com as grandes empresas multinacionais a operarem a partir de várias cidades do mundo e para várias cidades do mundo. Além disso, uma cidade inteligente desenvolvida e madura é uma cidade atrativa a novos investimentos, com capacidade para acolher grandes empresas multinacionais, o que ajuda a desenvolver economicamente uma cidade.

No entanto, não se pode analisar as vantagens sem olhar também para as dificuldades. De facto, apesar de o Parlamento Europeu e da Comissão Europeia trabalharem paralelamente para que haja cooperação entre os países-membros da União Europeia, existe na realidade uma divergência de ideias entre eles, o que pode pôr em causa a eficácia destas iniciativas. A título de exemplo, as novas regras sobre o uso da Inteligência Artificial na Europa que estão a ser discutidas neste momento¹⁶¹ no Parlamento Europeu, estão a ser alvo de alguma divergência entre os estados-membros, nomeadamente, em relação ao uso de dados pessoais recolhidos através das já referidas câmaras biométricas. Segundo Maria Graça Carvalho, eurodeputada no Parlamento Europeu, este último tem sido alvo de maiores controvérsias, no sentido de perceber a quem pertencem os dados, como são armazenados e em que situações somos obrigados a partilhá-los¹⁶². Este tema ainda é alvo de discórdia entre os países

¹⁶¹ Outubro de 2023.

¹⁶² CARVALHO, Maria Graça — **A Inteligência Artificial aplicada às Smart Cities**. Lisboa: Smart Cities Summit Portugal, 12 de outubro de 2023.

membros da União Europeia, uma vez que ainda não existe um consenso sobre as situações plausíveis de permitir a partilha de dados para a manutenção da segurança pública. Por exemplo, será que se torna viável a partilha destes dados em estado de calamidade? Ou ainda assim é algo que deve ser evitado a todo o custo? Estas questões permanecem no Parlamento Europeu e estão, à data, a ser debatidas. Prevê-se a sua conclusão no dia 25 de novembro de 2023 no Parlamento Europeu que, neste momento, está a discutir com a Comissão Europeia o melhor caminho a tomar. Ainda segundo Maria da Graça Carvalho, será provável que a decisão recaia sobre cada país sobre o uso ou não destes dados, uma vez que se trata de um assunto de segurança nacional. Não obstante, a divergência ficará espelhada nas decisões tomadas por cada país.

Por outro lado, o acesso desigual a tecnologias é um ponto a ter em consideração, uma vez que países com menos capacidade económica para ter acesso a tecnologia de ponta vão, inevitavelmente, ficar para trás e cavar um fosso maior entre países ricos e países pobres.

No entanto, o Parlamento Europeu e a Comissão Europeia trabalham juntos para a cooperação internacional, na medida em que facultam regulamentação e financiamento para as *smart cities* da União Europeia, de modo a que haja apoio para projetos inovadores e tecnológicos. Se Londres perdeu estes apoios aquando do *Brexit*, Amesterdão continua a ser apoiado nestas decisões, o que tem ajudado esta cidade a evoluir.

Em suma, tanto Londres e Amesterdão são dois bons exemplos de cidades inteligentes europeias que ajudam a que a Europa consiga competir com outras grandes cidades inteligentes mundiais, designadamente norte-americanas e asiáticas. Ainda existe um longo caminho a percorrer, no entanto, a cooperação internacional, apesar das suas lacunas, tem contribuído para que seja possível alavancar o desenvolvimento económico e tecnológico de grandes cidades europeias.

Conclusões

Este estudo permitiu chegar a algumas conclusões relativas ao atual dilema do direito à privacidade com a evolução das cidades inteligentes, tanto na análise do conhecimento da população em relação à circulação da sua informação no ciberespaço, como na análise de duas das cidades mais desenvolvidas da Europa neste plano, nomeadamente em Londres e Amesterdão.

Os resultados apresentados ao longo deste estudo revelam que ainda há uma falha muito grande nas estruturas de proteção da informação pessoal no ciberespaço e permitiram responder ao objetivo principal proposto relativamente à problemática que as cidades inteligentes trazem para o direito à privacidade. Embora a tecnologia venha em auxílio da população e com o objetivo de tornar a vida mais cómoda, a verdade é que esse objetivo acarreta consequências que nem todos os cidadãos estão dispostos a enfrentar: designadamente a vulnerabilidade dos seus dados pessoais. Por ser um caminho incontornável é importante que se estabeleçam mais leis que protejam esses dados e que apoiem os cidadãos quando a sua violação ocorrer. Para colmatar esta situação, foi também possível perceber que a Comissão Europeia, juntamente com o Parlamento Europeu, já estão a discutir estas vulnerabilidades e que, comparativamente com a China, estabelecem normas muito mais rígidas sobre a aplicação da IA, nomeadamente na vigilância das cidades, como foram referidas as câmaras biométricas.

Depois, ao analisar as cidades de Londres e Amesterdão, foi possível responder ao objetivo secundário deste estudo. Chegou-se à conclusão que Amesterdão, sendo uma cidade inteligente bastante desenvolvida, já se preocupa bastante com o tema da privacidade dos cidadãos relativamente ao recurso à IA, principalmente no que diz respeito ao quadro internacional, considerando urgente a cooperação e coesão de todos os países da União Europeia para que esta seja uma resposta que saia fortalecida.

Já Londres, embora esteja num nível de avanço tecnológico diferente e, talvez, superior, tem uma estratégia definida muito diferente da de Amesterdão e, por isso, as preocupações das duas cidades também divergem. Uma vez que o Reino Unido já não faz parte da União Europeia, Londres acaba por não se manifestar tanto no contexto da coesão internacional, muito embora a segurança dos seus cidadãos não seja colocada de lado.

Como foi possível concluir no decorrer desta investigação, as cidades inteligentes têm um grande impacto nas Relações Internacionais, não só por aquilo que significam, mas também pelo poder que advém deste tipo de cidades. A geopolítica está a mudar também no panorama do poder tecnológico que, hoje em dia, tem um peso muito grande na ordem mundial. Tal como foi analisado, as cidades inteligentes (e tanto Londres como Amesterdão o demonstram atualmente), não só são capazes de mudar a forma de cooperação com outras cidades, como sendo líderes globais na tecnologia, são bastante atraentes para a criação de novos negócios, *startups* e outras empresas de tecnologia que estão a crescer bastante em número. Tendo as infra-estruturas necessárias e mais favoráveis, as cidades inteligentes mais desenvolvidas são parte do ecossistema ideal para o desenvolvimento e inovação de novas empresas. A inovação aliada ao investimento são dois fatores cruciais para o desenvolvimento económico de uma cidade e, conseqüentemente, do seu país. Certamente que neste cenário será inevitável o surgimento de novos acordos políticos e económicos com outras cidades e entre países.

Relativamente aos desafios das cidades inteligentes colocam às Relações Internacionais, é possível nomear, por exemplo, as desigualdades entre países, a questão da segurança, incluindo a segurança humana nas suas sete dimensões, e a desvantagem competitiva dos países menos desenvolvidos. A segurança da proteção de dados é crucial também nas Relações Internacionais, até porque a legislação em cada país muitas vezes não coincide, o que coloca em causa a segurança de estrangeiros. Além disso, sendo o ciberespaço um espaço global, é necessários que potências como a União Europeia tenham já bem traçada a legislação em vigor no espaço europeu que, por sua vez, pode ou não ser motivo de discórdia. Manter uma União Europeia unida passa também por haver uma coesão e coerência entre os países-membros neste domínio.

Relativamente ao tema principal levantado por esta dissertação, a questão da privacidade e da segurança dos dados pessoais é um dos fatores mais sensíveis quando se fala em cidades inteligentes e IA. Considera-se, no entanto, que a investigação feita conseguiu chegar a uma resposta às questões levantadas: quais os desafios colocados no direito à privacidade no mundo do ciberespaço? De certo que existem inúmeros entraves e dilemas, nomeadamente na questão ética sobre que dados usar e não usar. Muito embora tenha ficado comprovado que a China, por exemplo, não se rege pelos mesmos padrões éticos que a

Europa e que, portanto, utiliza os dados privados dos cidadãos de uma forma muito mais leviana do que a Europa ou os EUA.

De facto, a análise dos casos de estudo de Londres e Amesterdão, comparando-as com outras cidades mundiais, ajudou à percepção da posição da Europa sobre este tema e daquilo que está a ser alcançado. O tema dos dados pessoais e a problemática da sua proteção é um tema recorrente no Parlamento Europeu e na Comissão Europeia, pelo que a cooperação internacional é um fator crucial na resolução destes casos.

Através do questionário, foi possível concluir que a maioria da população não está sequer consciente do impacto que a divulgação de dados na *internet* tem e muito menos dos perigos que isso acarreta. A maioria concorda que para poder usufruir das regalias da *internet* precisa de consentir a divulgação de dados, muito embora haja uma parte crescente da população que começa a ter em conta o peso que a divulgação dos dados tem e que tenta, cada vez mais, reduzir a informação pessoal que divulga. De facto, apesar de todos os avanços e recuos feitos pelo Parlamento Europeu e pela Comissão Europeia, o início da proteção de dados começa pela educação e pela consciencialização da população sobre os perigos que esta divulgação acarreta.

Em suma, esta investigação permitiu confirmar os objetivos, principal e secundário, propostos nesta dissertação de mestrado, no entanto, ainda há um grande caminho a percorrer tanto na instrução da população, como na maturação das infra-estruturas de segurança digital. Embora já seja um tema em debate, é certo que a proteção de dados digitais ainda requer muita atenção, tanto por cada país individualmente, como a nível internacional, o que, devido ao carácter global e sem fronteiras do espaço digital, nunca poderá ser desconsiderado. Por este motivo, esta é uma questão em aberto e com espaço para futuros estudos e análises.

Referências Bibliográficas

- Agência Lusa — **China garante que "nunca pediu" dados dos utilizadores do TikTok. E diz estar a ser alvo de “perseguição política alimentada pela xenofobia”** [Em linha]. Lisboa: CCN, 2023. [Consultado em 26-03-2023]. Disponível em: <https://cnnportugal.iol.pt/china/tiktok/china-garante-que-nunca-pediu-dados-dos-utilizadores-do-tiktok-e-diz-ser-alvo-de-perseguiacao-politica-alimentada-pela-xenofobia/20230324/641d7ce10cf2665294dbb0f7>.
- AGUIAR, Miguel — **O Digital ao Serviço da Saúde: da Telemedicina à Medicina ao Domicílio: Necessidades e Oportunidades a Nível Local**. Lisboa: Smart Cities Summit Portugal, 12 de outubro de 2023.
- ALBERTS, Gerard [*et al.*] — Archaeology of the Amsterdam digital city; why digital data are dynamic and should be treated accordingly. **Internet Histories** [Em linha]. 1:1-2 (2017) 146-159. [Consultado em 16-03-2022]. Disponível em: https://www.researchgate.net/publication/321323674_Archaeology_of_the_Amsterdam_digital_city_why_digital_data_are_dynamic_and_should_be_treated_accordingly.
- Amsterdam Smart City — **Amsterdam Economic Board** [Em linha]. Disponível em: <https://amsterdamsmartcity.com/> [Consultado em 02-11-2022].
- BALL, James — **The real story of Cambridge Analytica and Brexit** [Em linha]. Reino Unido: The Spectator, 2020. [Consultado em 27-05-2023]. Disponível em: <https://www.spectator.co.uk/article/were-there-any-links-between-cambridge-analytica-russia-and-brexit/>.
- BING, Li — Effective energy utilization through economic development for sustainable management in smart cities. **Energy Reports** [Em linha]. vol.8 (2022) 4975-4987. [Consultado em 08-10-2023]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2352484722005480>.
- Bloomberg — **Banco central da Rússia quer proibir mineração e comércio de criptomoedas** [Em linha]. Lisboa: Económico Valor, 2022. [Consultado em 09-09-2022]. Disponível em: <https://valor.globo.com/financas/noticia/2022/01/20/banco-central-da-russia-quer-proibir-mineracao-e-comercio-de-criptomoedas.ghtml>.

- BORGES, João Vieira [et al.] — **Ameaças e Riscos Transnacionais no Novo Mundo Global**. Porto: Fronteira do Caos Editores LDA, 2016. ISBN: 978-989-8647-60-3.
- Bright Cities — **Mapa Mundial de cidades inteligentes: Taipei** [Em linha]. In Bright Cities, sd. [Consultado em 28-04-2023]. Disponível em: <https://www.brightcities.city/smart-city-profile/Taipei-NorthernTaiwan-Taiwan/5bde2ada3f9f3d37162cada3>.
- CADWALLADR, Carole; GRAHAM-HARRISON, Emma — **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach** [Em linha]. Reino Unido: The Guardian, 2018. [Consultado em 05-04-2023]. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- CARRIER, Frédérique — **How are Smart Cities meeting the challenges of urbanization in the 21st century?** [Em linha]. In RBC Wealth Management, sd. [Consultado em 02-02-2022]. Disponível em: <https://www.rbcwealthmanagement.com/en-us/insights/how-are-smart-cities-meeting-the-challenges-of-urbanization-in-the-21st-century>.
- CARVALHO, Maria Graça — **A Inteligência Artificial aplicada às Smart Cities**. Lisboa: Smart Cities Summit Portugal, 12 de outubro de 2023.
- CCDCOE — **Our mission & Vision** [Em linha]. In CCDCOE, sd. [Consultado em 30-10-2023]. Disponível em: <https://ccdcoe.org/about-us/>.
- CHIN, Bernice — **Inside Smart City Taiwan: A New Solution for Urban Living** [Em linha]. Taiwan: Hive Live, 2021. [Consultado em 15-10-2022]. Disponível em: <https://hivelife.com/smart-city-taiwan/>.
- City Innovation Experiment Lab — **Camara Vision Experiment** [Em Linha]. Amesterdão, 2022. [Consultado em 02-11-2022]. Disponível em: <https://www.citixl.com/living-labs/we-make-the-city-festival/>.
- Conselho Europeu — **Declaração Conjunta sobre a cooperação UE-OTAN, 10 de janeiro de 2023** [Em linha]. Bruxelas: Conselho Europeu, 2023. [Consultado em 04-10-2023]. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/>.
- Comissão Europeia — **Índice de Economia e Sociedade Digitais (DESI)** [Em linha]. Bruxelas: Comissão Europeia, sd. [Consultado a 07-04-2023]. Disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/desi>.

- Comissão Europeia — **Orientações para a Digitalização até 2030: a via europeia para a Década Digital** [Em linha]. Bruxelas: Comissão Europeia, 2021. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021DC0118&from=de>.
- COOKSON, Clive; PARKER, George — **UK to invest £2.5bn in quantum computing drive** [Em linha]. Reino Unido: Financial Times, 2023. [Consultado em 30-04-2023]. Disponível em: <https://www.ft.com/content/900ba4ee-6c60-4406-963a-810771c2ad7c>.
- CRANMER, Elenor E. [*et al.*] — Internet of Things: Aspiration, implementation and contribution. **Journal of Business Research** [Em linha]. vol.139 (2022) 69-80, ISSN 0148-2963. [Consultado em 16-03-2022]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0148296321006706>.
- CSUKÁ, Máté S.; SZABÓ, Roland Z. — The many faces of the smart city: Differing value propositions in the activity portfolios of nine cities. **Cities** [Em linha]. Volume:112 (2021) 103-116. [Consultado em 17-06-2021]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0264275121000147>. ISSN 0264-2751.
- DAMIÃO, Rui — **O que se sabe (até ao momento) sobre o ciberataque à Vodafone** [Em linha]. Lisboa: IT Security, 2022. [Consultado em 19-10-2022]. Disponível em: <https://www.itsecurity.pt/news/x-ray/o-que-se-sabe-ate-ao-momento-sobre-o-ciberataque-a-vodafone>.
- DN/Lusa — **China condena pressão exercida pelos Estados Unidos sobre Portugal** [Em linha]. Lisboa: Diário de Notícias, 2020. [Consultado em 03-03-2023]. Disponível em: <https://www.dn.pt/mundo/china-condena-pressao-exercida-pelos-estados-unidos-sobre-portugal-12909061.html>.
- DZIEWANOWSKI, Jacek — AQAP Inspire Magazine as a tool motivating to terrorist activities. **Internal Security Review** [Em linha]. 20/10 (2019) pp. 339-352. [Consultado em 22-05-2023]. Disponível em: https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-ece248ec-620e-476a-8473-41ed81d574a0/c/Dziewanowski_-_ANG.pdf.
- ELIAS, Luís — Criminalidade Transnacional Organizada. Paradoxos Conceptuais e Desafios Políticos e Operacionais. In BORGES, João Vieira [*et al.*] — **Ameaças e Riscos**

- Transnacionais no Novo Mundo Global**. Porto: Fronteira do Caos Editores LDA, 2016. ISBN: 978-989-8647-60-3.
- European Commission, Directorate-General for Research and Innovation — **Industry 5.0: human-centric, sustainable and resilient** [Em linha]. In Publications Office, 2021. [Consultado em 09-02-2022]. Disponível em: <https://data.europa.eu/doi/10.2777/073781>.
- European Commission — **The Cybersecurity Strategy** [Em linha]. Bruxelas: European Commission, 2022. [Consultado em 21-09-2022]. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>.
- European Commission — **Reflection Paper: Towards a Sustainable Europe by 2030** [Em linha]. Bruxelas: European Commision, 2019. [Consultado em 6-02-2023]. Disponível em: https://commission.europa.eu/system/files/2019-02/rp_sustainable_europe_30-01_en_web.pdf.
- European Innovation Council — **The European Capital of Innovation Award** [Em linha]. Bruxelas: European Innovation Council, 2022. [Consultado em 02-11-2022]. Disponível em: https://eic.ec.europa.eu/eic-funding-opportunities/eic-prizes/european-capital-innovation-awards_en.
- Europol — **International operation closes down Piilopuoti dark web marketplace** [Em linha]. In Europol, 2023. [Consultado a 30-09-2023]. Disponível em: <https://www.europol.europa.eu/media-press/newsroom/news/international-operation-closes-down-piilopuoti-dark-web-marketplace>.
- Europol — **Netherlands, France and Estonia win the 2023 Europol Excellence Awards in Innovation** [Em linha]. In Europol, 2023. [Consultado em 30-09-2023]. Disponível em: <https://www.europol.europa.eu/media-press/newsroom/news/netherlands-france-and-estonia-win-2023-europol-excellence-awards-in-innovation>.
- FAN, Wu — **Smart Cities Deep Dive: AI-Powered Urbanization** [Em linha]. In China Talk, 2023. [Consultado em 10-10-2023]. Disponível em: <https://www.chinatalk.media/p/smart-cities-deep-dive-ai-powered>.
- FREITAS, João Abel de — **A Nova Rota da Seda** [Em linha]. Lisboa: O Jornal Económico, 2021. [Consultado a 20-05-2023]. Disponível em: <https://jornaleconomico.pt/noticias/a-nova-rota-da-seda-719446/>.

- FRENKEL, Sheera — **The storming of Capitol Hill was organized on social media** [Em linha]. In *The New York Times*, 2021. [Consultado em 25-05-2023]. Disponível em: <https://www.nytimes.com/2021/01/06/us/politics/protesters-storm-capitol-hill-building.html>.
- GlobalData Thematic Research — **History of smart cities: Timeline** [Em linha]. In *Verdict*, 2020. [Consultado em 07-02-2022]. Disponível em: <https://www.verdict.co.uk/smart-cities-timeline/>.
- GOODE, Lauren — **Review: We Put ChatGPT, Bing Chat, and Bard to the Test** [Em linha]. In *Wired*, 2023. [Consultado em 04-05-2023]. Disponível em: <https://www.wired.com/story/review-ai-chatbots-bing-bard-chat-gpt/>.
- Greater London Authority — **The Spatial Development Strategy For Greater London** [Em linha]. Londres: The London Plan, 2021. [Consultado em 20-10-2022]. Retirado de: https://www.london.gov.uk/sites/default/files/the_london_plan_2021.pdf.
- HACKETT, Paul — **Following the crowd: Amsterdam's smart city solution** [Em linha]. In *EuroNews*, 2021. [Consultado em 18-11-2022]. Disponível em: <https://www.euronews.com/next/2021/08/27/following-the-crowd-amsterdam-s-smart-city-solution>.
- Hang, N. T. T. — The Rise of China: Challenges, Implications, and Options for the United States. **Indian Journal of Asian Affairs** [Em linha]. 30:1/2, (2017) pp. 47–64. [Consultado em 21-08-2023]. Disponível em: <http://www.jstor.org/stable/26465816>.
- Hellman Electric — **Big Apple, Smart City. How New York Is Fast Becoming the Greatest Smart City in the World** [Em linha]. In Hellman Electric, 2019. [Consultado em 09-10-2023]. Disponível em: https://hellmanelectric.com/wp-content/uploads/2019/06/Hellman_SmartCities_NewYork_eBook_FINAL.pdf.
- HERZOG, Stephen — Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security** [Em linha]. 4:2 (2011) Strategic Security in the Cyber Age, pp. 49-60. [Consultado em 03-03-2023]. Disponível em: <https://www.jstor.org/stable/26463926?seq=10>.
- HM Government — **Government Cyber Security Strategy: Building a cyber resilient public sector** [Em linha]. Londres: HM Government, sd. [Consultado em 20-04-2023].

- Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf.
- HOWELL, Sam — **The China-US Quantum Race: In the quantum race, second place may be the first to lose** [Em linha]. In *The Diplomat*, 2023. [Consultado em 30-04-2023]. Disponível em: <https://thediplomat.com/2023/01/the-china-us-quantum-race/>.
- IDN-CESEDEN — **Estratégia da Informação e Segurança no Ciberespaço** [Em linha]. In *idn cadernos*, 2013. [Consultado em 05-03-2023]. Disponível em: https://www.idn.gov.pt/publicacoes/idncadernos/Documents/2013/idncaderno_12.pdf.
- I. Iberty — **The Human Rights Act** [Em linha]. Londres: I. Iberty, 2022. [Consultado em 02-11-2022]. Disponível em: <https://www.libertyhumanrights.org.uk/your-rights/the-human-rights-act/>.
- I. Liberty — **A Private and Family Life** [Em linha]. Londres: I. Iberty, 2022. [Consultado em 02-11-2022]. Disponível em: <https://www.libertyhumanrights.org.uk/right/a-private-and-family-life/>.
- Information Commissioner's Office — **Data Protection by design and default** [Em linha]. In *Information Commissioner's Office*, sd. [Consultado em 02-11-2022]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#dpd12>.
- Jornal Oficial da União Europeia — **A Carta dos Direitos Fundamentais da União Europeia: Artigo 8.º** [Em linha]. [Consultado em 16-03-2022]. Disponível em: <https://fra.europa.eu/pt/eu-charter/article/8-proteccao-de-dados-pessoais>.
- KAKU, Michio — **Supremacia Quântica**. Lisboa: Editora Bertrand, 2023. ISBN: 978-972-25-4585-3.
- KISSINGER, Henry — **A Ordem Mundial: Reflexões sobre o carácter das Nações e o Curso da História**. D. Quixote: Alfragide, 2017, 4.ª edição. ISBN: 978-972-20-5623-6.
- KUYPER, Tijn — **City Highlight: Amsterdam** [Em Linha]. In *Medium*, 2019. [Consultado em 18-11-2022]. Disponível em: <https://medium.datadriveninvestor.com/city-highlight-amsterdam-ce3bdf6334b9>.

- London Data Source — **London's Population** [Em linha]. In London Data Source, sd. [Consultado em 20-11-2022]. Disponível em: <https://data.london.gov.uk/dataset/londons-population>.
- LORIMER, Stephan — How our plans for Smart London compare to other world cities [Em linha]. London: Smart London, 2018. [Consultado em 08-12-2022]. Disponível em: <https://chiefdigitalofficer4london.medium.com/the-vision-for-smart-london-and-how-it-compares-to-other-world-cities-8c5bbde903b5>.
- MALLERET, Constance; MILMO, Dan & HERN, Alex — **Pro-Bolsonaro violence: experts highlight role of social media platforms** [Em linha]. In The Guardian, 2023. [Consultado em 25-05-2023]. Disponível em: <https://www.theguardian.com/world/2023/jan/09/pro-bolsonaro-violence-social-media-platforms>.
- MARCELINO, Valentina — **Ciberataques. "São mais um espelho da ineficácia da organização atual das Forças Armadas"** [Em linha]. Lisboa: Diário de Notícias, 2022. [Consultado em 06-10-2022]. Disponível em: <https://www.dn.pt/politica/ciberataques-sao-mais-um-espelho-da-ineficacia-da-organizacao-atual-das-forcas-armadas-15218369.html>.
- Mayor Of London — **An Emerging Technology Charter for London** [Em linha]. Londres, 2021, atual. fevereiro 2022. [Consultado em 15-10-2022]. Disponível em: <https://www.london.gov.uk/publications/emerging-technology-charter-london>.
- Microsoft — **Ciberataques de Estado-nação se tornam mais ousados à medida que líderes autoritários escalam a agressão** [Em linha]. In Microsoft, 2022. [Consultado em 20-11-2022]. Disponível em: <https://news.microsoft.com/pt-br/ciberataques-de-estado-nacao-se-tornam-mais-ousados-a-medida-que-lideres-autoritarios-escalam-a-agressao/>.
- Ministério Público de Portugal — **Convenção de Genebra para melhorar a situação dos feridos e doentes das forças armadas em campanha** [Em linha]. Lisboa: Ministério Público, sd. [Consultado em 28-09-2023]. Disponível em: <https://www.idn.gov.pt/pt/formacao/educacao/recursos/Documents/Direitos%20Humanos%20e%20Direito%20Internacional%20Humanitário/I%20Convenção%20de%20Genebra%20sobre%20Conflitos%20Armados.pdf>.

- MORNINGSTAR, Murohy — **Washington** [Em linha]. In About Smart Cities, 2021. [Consultado em 08-10-2023]. Disponível em: <https://www.aboutsmartcities.com/smart-city-washington/>.
- MORRISON, Ryan — **Hackers increasingly targeting Internet of Things devices** [Em linha]. In Tech Monitor, 2022. [Consultado em 08-11-2022]. Disponível em: <https://techmonitor.ai/technology/cybersecurity/hackers-targeting-internet-of-things-devices>.
- Natalie — **ChatGPT — Release Notes** [Em linha]. In OpenAI, 2023. [Consultado em 06-06-2023]. Disponível em: <https://help.openai.com/en/articles/6825453-chatgpt-release-notes>.
- NUNES, Paulo — Ciberameaças e quadro legal dos conflitos no ciberespaço. In BORGES, João Vieira [et al.] — **Ameaças e Riscos Transnacionais no Novo Mundo Global**. Porto: Fronteira do Caos Editores LDA, 2016. ISBN: 978-989-8647-60-3.
- NYPD — **NYPD Announces Citywide Crime Statistics for June 2023** [Em linha]. In NYPD Media Report, 2023. [Consultado em 11-10-2023]. Disponível em: <https://www.nyc.gov/site/nypd/news/p00084/nypd-citywide-crime-statistics-june-2023>.
- ONU — **Carta das Nações Unidas** [Em linha]. In ONU, sd. [Consultado em 28-09-2023]. Disponível em: <https://www.cig.gov.pt/wp-content/uploads/2018/01/Carta-das-Nações-Unidas.pdf>.
- OTTIS, Rain — Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective [Em linha]. In OCCDCOE, 2008. [Consultado em 03-03-2023]. Disponível em: https://ccdcocoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
- Parlamento Europeu — **Parlamento negocia primeiras regras para inteligência artificial mais segura** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2023. [Consultado em 04-10-2023]. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20230609IPR96212/parlamento-negocia-primeiras-regras-para-inteligencia-artificial-mais-segura>.
- Parlamento Europeu — **Prioridades e contributos do Parlamento Europeu** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2023. [Consultado em 04-10-2023]. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/press-tool-kit/1/prioridades-politicas-do-parlamento-europeu-para-2023>.

- Parlamento Europeu — **Serviços digitais: novas regras para um ambiente em linha mais seguro e aberto** [Em linha]. Lisboa: Atualidade Parlamento Europeu, 2022. [Consultado em 04-10-2023]. Disponível em: <https://www.europarl.europa.eu/news/pt/press-room/20220701IPR34364/servicos-digitais-novas-regras-para-um-ambiente-em-linha-mais-seguro-e-aberto>.
- PINTO, Pedro — **Conversas Globais: as grandes questões geopolíticas, nacionais e internacionais**. Lisboa: Bertrand Editora, 2020. ISBN: 978-972-25-3805-3.
- POLITOU, Eugenia [*et al.*] — Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. **Journal of Cybersecurity** [Em linha]. 4:1 (2018) pp. 1-20. [Consultado em 09-10-2022]. Disponível em: <https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056>.
- Press Releases — **Vodafone Portugal alvo de ciberataque** [Em linha]. In Vodafone, 2022. [Consultado em 20-10-2022]. Disponível em: <https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html>.
- Prisha — **Eight-year-old boy orders an AK-47 from dark web, gets it delivered to home** [Em linha]. In Wion, 2023. [Consultado em 03-10-2023]. Disponível em: <https://www.wionews.com/trending/eight-year-old-boy-orders-an-ak-47-from-dark-web-gets-it-delivered-to-home-620186>.
- Privacy City of Amsterdam — **Cameras, Sensors and your privacy** [Em Linha]. In Amsterdam, sd. [Consultado em 18-11-2022]. Disponível em: <https://www.amsterdam.nl/privacy/camera-sensoren-privacy/>.
- PUTTKAMER, Laura — **Interview with Chat GPT on the Smart City** [Em linha]. In Bee Smart City, 2023. [Consultado a 04-05-2023]. Disponível em: <https://www.beesmart.city/en/strategy/interview-with-chat-gpt-on-the-smart-city>.
- REGAN, Emma — **Smart Cities in Japan: Practical Innovations for Conscious Future Living** [Em linha]. In Tokyo-esque, 2022. [Consultado em 30-04-2023]. Disponível em: <https://tokyo-esque.com/smart-cities-in-japan/>.
- Register of Commission Documents — **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)** [Em linha]. Bruxelas: Comissão Europeia, 2020.

- [Consultado em 18-11-2022]. Disponível em: [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2020\)767&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)767&lang=en).
- SANGER, David E. — **A Arma Perfeita: guerra, sabotagem e medo na Era da cibersegurança**. Lisboa: Casa das Letras, 2021. ISBN: 978-989-66-1122-4.
- SAVAGE, Michael — **How Brexit party won Euro elections on social media – simple, negative messages to older voters** [Em linha]. In *The Guardian*, 2019. [Consultado a 27-05-2023]. Disponível em: <https://www.theguardian.com/politics/2019/jun/29/how-brexit-party-won-euro-elections-on-social-media>.
- SCHAPPERT, Stefanie — **Millions of personal data stolen by ethical hacker still floating around dark web** [Em linha]. In *cybernews*, 2023. [Consultado em 03-10-2023]. Disponível em: <https://cybernews.com/news/ransomware-ethical-hacker-steals-millions-personal-data-dark-web/>.
- SCHEIDER-PETSINGER, Marianne [et al.] — **US–China Strategic Competition. The Quest for Global Technological Leadership** [Em linha]. In *Americas Programme*, 2019. [Consultado em 21-08-2023]. Disponível em: <https://www.chathamhouse.org/sites/default/files/CHHJ7480-US-China-Competition-RP-WEB.pdf>.
- Sem autor — **2007 cyber attacks on Estonia** [Em linha]. In *Cyber operations*, sd. [Consultado em 13-09-2022] Disponível em: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.
- Sem autor — **Back End - Dries Depoorter** [Em linha]. In *MU*, sd. [Consultado em 09-03-2022]. Disponível em: <https://www.mu.nl/en/exhibitions/back-end-dries-depoorter>.
- Sem autor — **Cisco garante que ciberataque não impactou negócio e serviços** [Em linha]. In *IT Security*, 2022. [Consultado em 21-10-2022]. Disponível em: <https://www.itsecurity.pt/news/news/cisco-garante-que-ciberataque-nao-impactou-negocio-e-servicos>.
- Sem autor — **Identificação e dados biométricos, sabe o que são?** [Em linha]. In *Notas em Dia*, 2023. [Consultado em 04-10-2023]. Disponível em: https://www.notasemdia.pt/vida-mais-simples/identificacao-e-dados-biometricos-sabe-o-que-sao/?gclid=Cj0KCQjwmvSoBhDOARIsAK6aV7gbIK3T3S1tufruLyt4wjEzqRA-pcpQSF0LHbyjzHpj6brG8lqTAk4aApO3EALw_wcB.

- Sem autor — **International police arrest 288 worldwide in dark web bust** [Em linha]. In DutchNews, 2023. [Consultado em 03-10-2023]. Disponível em: <https://www.dutchnews.nl/2023/05/international-police-arrest-288-worldwide-in-dark-web-bust/>.
- Sem autor — **New Taipei mobile payment (NewTaiPAY) combined with New Taipei coin will be launched in July** [Em linha]. In Smart New Taipei City, 2023. [Consultado em 07-10-2023]. Disponível em: <https://smartcity.ntpc.gov.tw/en/home.jsp?id=8776589f27d974f8&act=be4f48068b2b0031&dataserno=7c465005118585aff7a3952d1ba8b1ce>.
- Sem autor — **Smart Cities Around the World: Amsterdam Edition** [Em linha]. In GovTech Singapore, 2021. [Consultado em 09-08-2023]. Disponível em: <https://www.tech.gov.sg/media/technews/smart-cities-around-the-world-amsterdam>.
- Sem autor — **Smart Cities Supporting tech-enabled urban development to solve the most pressing challenges facing NYC and the world** [Em linha]. In NYCEDC, s.d. [Consultado em 11-10-2023]. Disponível em: <https://edc.nyc/industry/smart-cities>.
- Sem autor — **Smart City-2023 NTPC International Smart City Forum** [Em linha]. In Smart New Taipei City, 2023. [Consultado em 07-10-2023]. Disponível em: <https://smartcity.ntpc.gov.tw/en/home.jsp?id=8776589f27d974f8&act=be4f48068b2b0031&dataserno=c2a57819c8512d55b36475fba62abel1a>.
- Sem autor — **The Dutch Digital Strategy** [Em linha]. In Sem local, 2021. [Consultado em 28-10-2022]. Disponível em: <https://www.nederlanddigitaal.nl/binaries/nederlanddigitaal-nl/documenten/publicaties/2021/06/22/the-dutch-digitalisation-strategy-2021-eng/210621-min-ezk-digitaliseringstrategie-en-v03.pdf>.
- Sem autor — **What is LoRaWAN?** [Em linha]. In Caburn Telecom, sd. [Consultado a 08-11-2023]. Disponível em: https://caburntelecom.com/what-is-lorawan/?gad_source=1&gclid=Cj0KCQiAgK2qBhCHARIsAGACuzmqVQWFQFfyZPYE9lPt5KuruvLLvq8EET4-FlucCXLJRl8d5jU2xjUaAm0VEALw_wcB.
- SMITH, Lisa — **Amsterdam Smart City: A World Leader in Smart City Development** [Em linha]. In Bee Smart City, 2017. [Consultado a 05-05-2023]. Disponível em: <https://www.beesmart.city/city-portraits/smart-city-portrait-amsterdam>

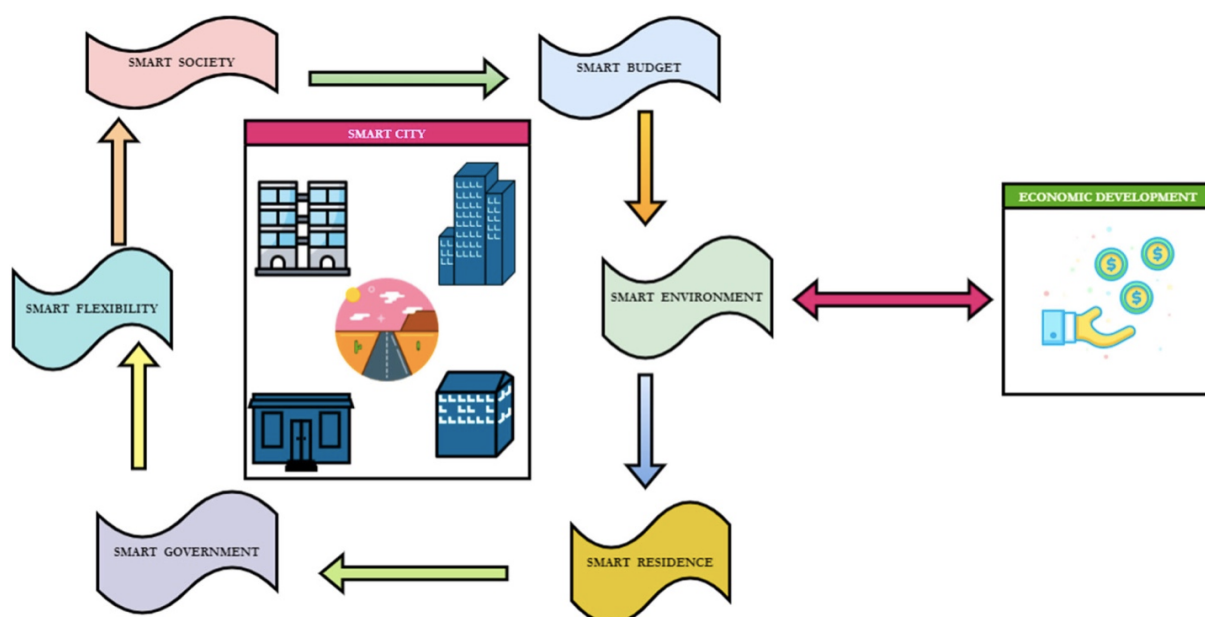
- Statista — **Total population of Amsterdam from 2009 to 2022** [Em linha]. In Statista, sd. [Consultado em 20-11-2022]. Disponível em: <https://www.statista.com/statistics/753235/total-population-of-amsterdam/>.
- The United States Department of Justice — **Global Disruption of Three Terror Finance Cyber-Enabled Campaigns** [Em linha]. In Office of Public Affairs, 2020. [Consultado a 25-05-2023]. Disponível em: <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.
- TOBIAS, Michael — **How New York is Becoming a Smart City** [Em linha]. In Nearby Engineers, s.d. [Consultado a 11-10-2023]. Disponível em: <https://www.ny-engineers.com/blog/how-new-york-is-becoming-a-smart-city>.
- Too Gethr — **Simplify Parking** [Em linha]. In Too Gethr, sd. [Consultado em 30-10-2022]. Disponível em: <https://www.toogethr.com/en/parking>.
- TINNIRELLO, Maurizio — The Global Politics of Artificial Intelligence. ULNICANE, Inga [et al.] — **Governance of Artificial Intelligence: Emerging International Trends and Policy Frames** [Em linha]. CRC Press: London, 2022. [Consultado em 07-05-2022]. Disponível em: <https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9780429446726-2/governance-artificial-intelligence-inga-ulnicane-william-knight-tonii-leach-bernd-carsten-stahl-winter-gladys-wanjiku>. ISBN: 9780429446726.
- United Nations — **Human Security Handbook. An integrated approach for the realization of the Sustainable Development Goals and the priority areas of the international community and the United Nations system** [Em linha]. In United Nations Trust Fund For Human Security, 2016. [Consultado em 01-11-2023]. Disponível em: <https://www.un.org/humansecurity/wp-content/uploads/2017/10/h2.pdf>.
- XINHUA — **East China lab to get world-leading quantum computer** [Em linha]. In China Daily, 2023. [Consultado em 30-04-2023]. Disponível em: <https://www.chinadaily.com.cn/a/202303/08/WS6407d466a31057c47ebb2f6e.html>.
- YANGQIU, Chen; NING, Lai; XUETING, Zhang — China's City of the Future: Xiong'an New Area. **Innovations to Improve People's Quality of Life** [Em linha]. 70:1 (2021). [Consultado em 07-10-2023]. Disponível em: https://www.hitachi.com/rev/archive/2021/r2021_01/gir/index.html.

- YASAR, Kinza; LOSHIN, Peter; LUTKEVICH, Ben — **Definition data center** [Em linha].
In TechTarget, 2022. [Consultado em 07-10-2023]. Disponível em: [https://
www.techtarget.com/searchdatacenter/definition/data-center](https://www.techtarget.com/searchdatacenter/definition/data-center).
- YOUNG, Philip [*et al.*] — **London: A Global Leader in Advanced Digital Technologies**
[Em linha]. In Catapult Digital, Londres, 2020. [Consultado em 15-10-2022]. Retirado
de: [https://www.digicatapult.org.uk/wp-content/uploads/2020/07/DC_-_
_London_Advanced_Digital_Tech_Report_-_2020__1_.pdf](https://www.digicatapult.org.uk/wp-content/uploads/2020/07/DC_-_London_Advanced_Digital_Tech_Report_-_2020__1_.pdf).

Anexos

Anexo 1

Desenvolvimento Económico Sustentável



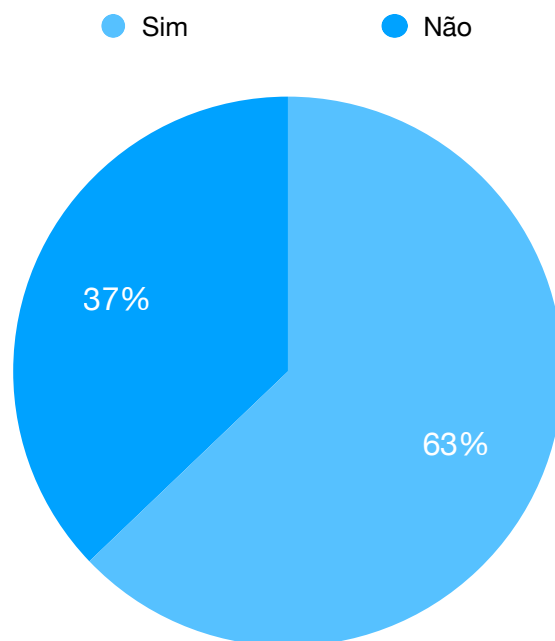
Fonte: BING, Li — Effective energy utilization through economic development for sustainable management in smart cities. *In Energy Reports*, vol.8, pp. 4975-4987, novembro de 2022.

Anexo 2

Lista de questões presentes no questionário elaborado

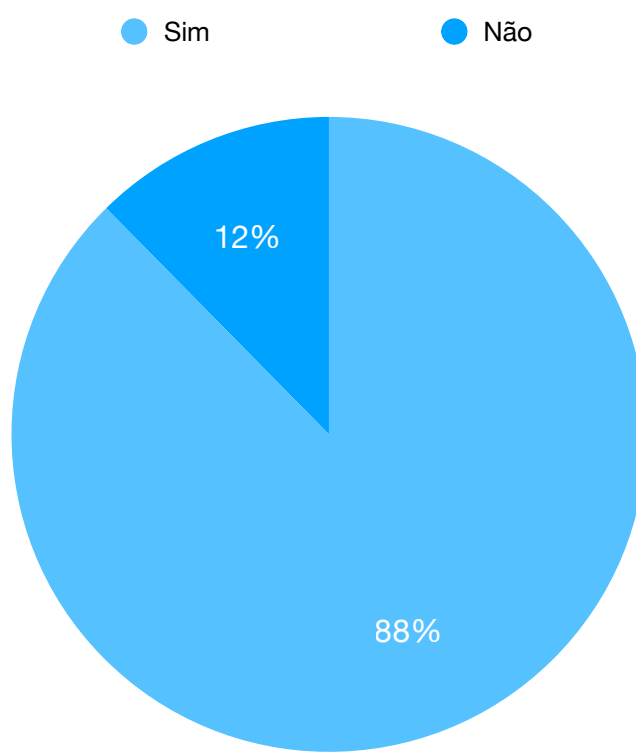
Questões
Qual é o teu género?
Qual é a tua idade?
Qual é a tua área de estudo/trabalho?
Recorres muitas vezes à <i>Internet</i> na tua profissão?
Na perspectiva de utilizador, qual o teu nível de conhecimento a nível informático?
Sabes o que são <i>HTTP Cookies</i> e para que servem?
Sabes o que é a <i>deep web</i> e a <i>dark web</i> ?
Sentes-te seguro/a ao inserires os teus dados pessoais em qualquer tipo de <i>website</i> ?
Consideras que abdicas demasiado dos teus direitos de privacidade para poderes utilizar a <i>Internet</i> ?
Consideras que em algumas plataformas te pedem demasiada informação pessoal?
Se sim, como é que isso te faz sentir?
Conheces o termo <i>ciberespaço</i> ?
Se sim, consideras o ciberespaço um espaço seguro?
Estás consciente que a tua informação pessoal pode circular no ciberespaço sem o teu consentimento?
Que medidas usas para proteger a tua informação pessoal no ciberespaço?
Qual a tua opinião sobre conectar digitalmente todos os dispositivos electrónicos?
Receias que a digitalização das atividades dos vários dispositivos do dia a dia coloque em risco a tua privacidade?

Resultados da resposta à questão:
“Sabes o que são *HTTP Cookies* e para que servem?”



Fonte: Questionário realizado pela autora.

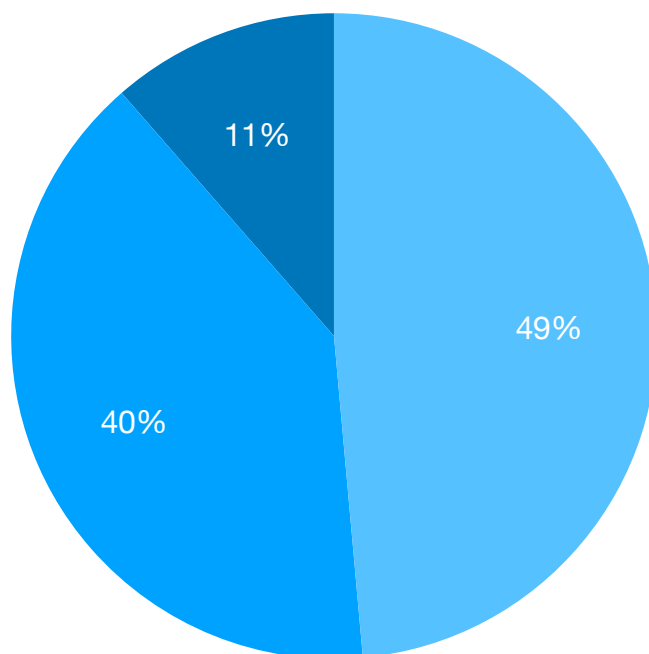
Resultados da resposta à questão:
“Sabes o que é a *deep web* e a *dark web*?”



Fonte: Questionário realizado pela autora.

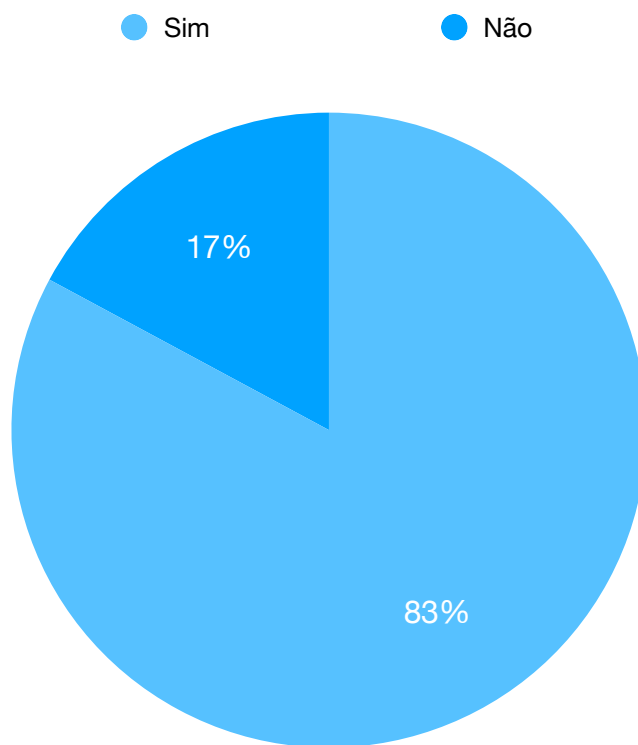
Resultados da resposta à questão:
“Conheces o termo *ciberespaço*?”

● Sim ● Já ouvi falar, mas não sei ao certo
● Não, nunca ouvi falar



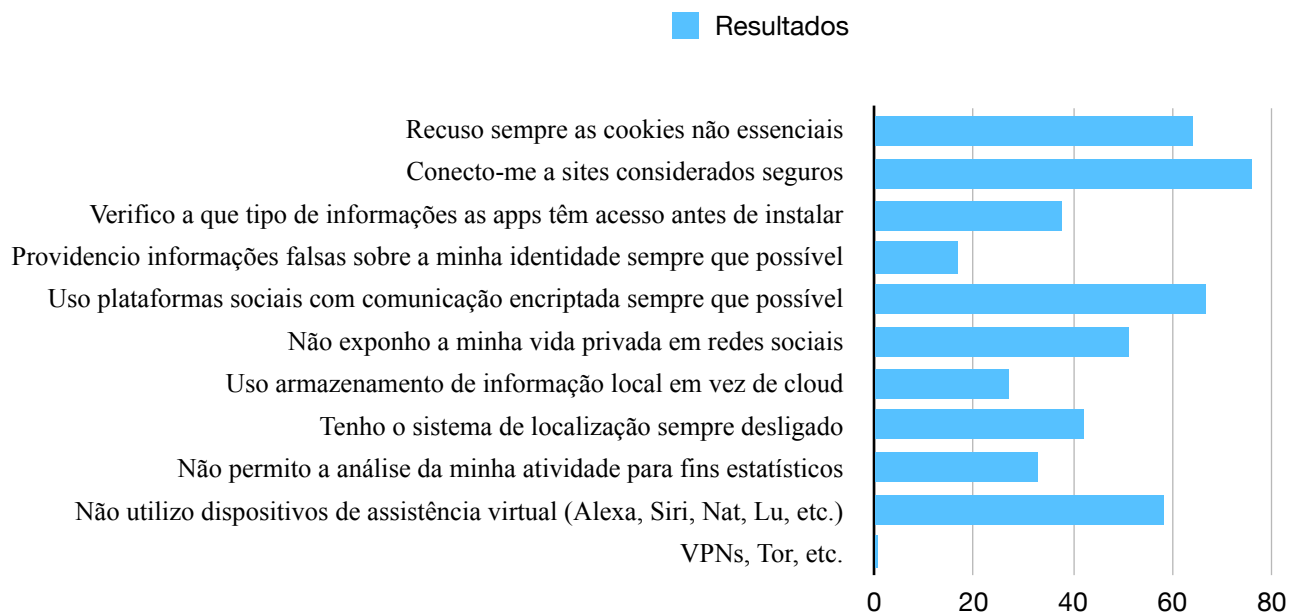
Fonte: Questionário realizado pela autora.

Resultados da resposta à questão:
“Estás consciente que a tua informação pessoal pode circular no ciberespaço
sem o teu consentimento?”



Fonte: Questionário realizado pela autora.

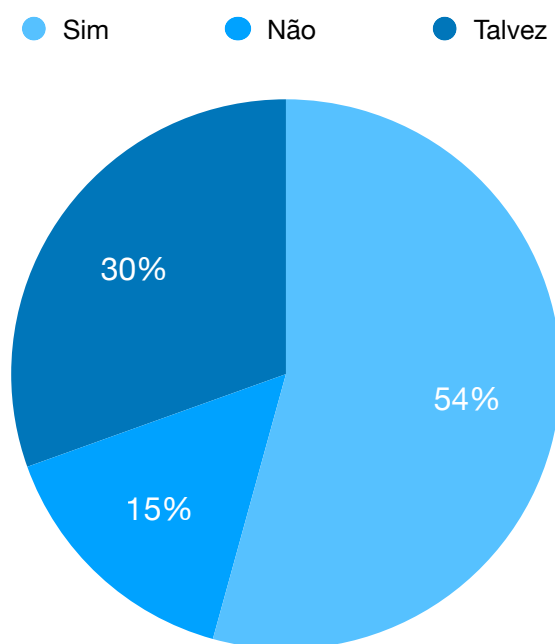
Resultados da resposta à questão presente no questionário relativo às medidas de segurança adotadas



Fonte: Questionário realizado pela autora.

Resultados da resposta à questão:

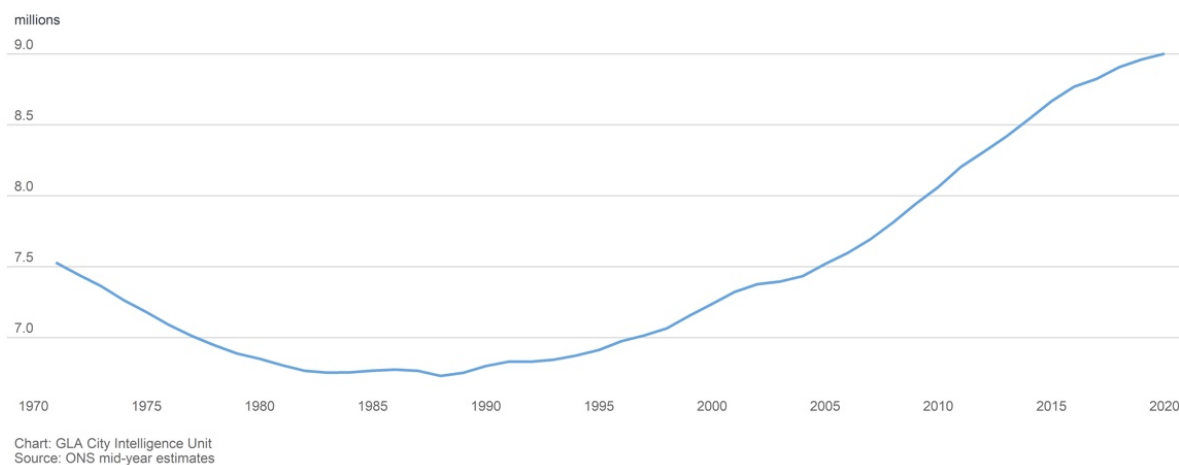
“Receias que a digitalização das atividades dos vários dispositivos do dia a dia coloque em risco a tua privacidade?”



Fonte: Questionário realizado pela autora.

Anexo 3

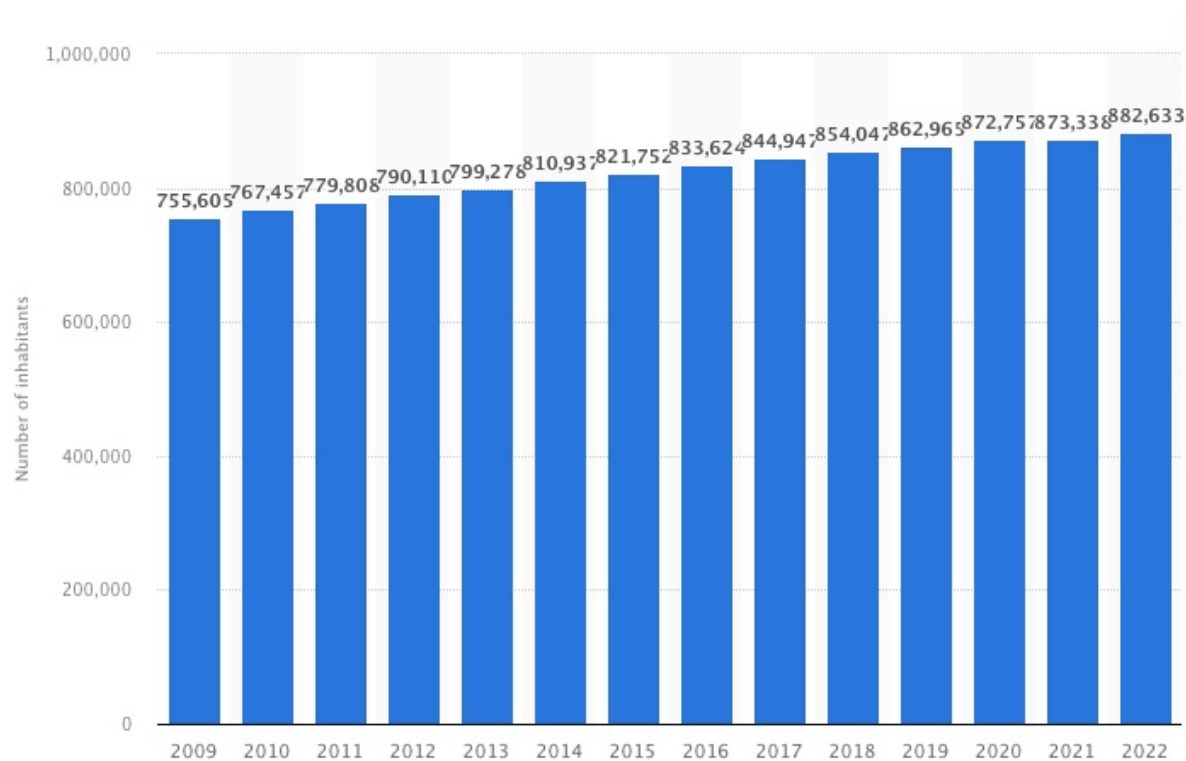
População de Londres 1971-2020



Fonte: London Data Source.

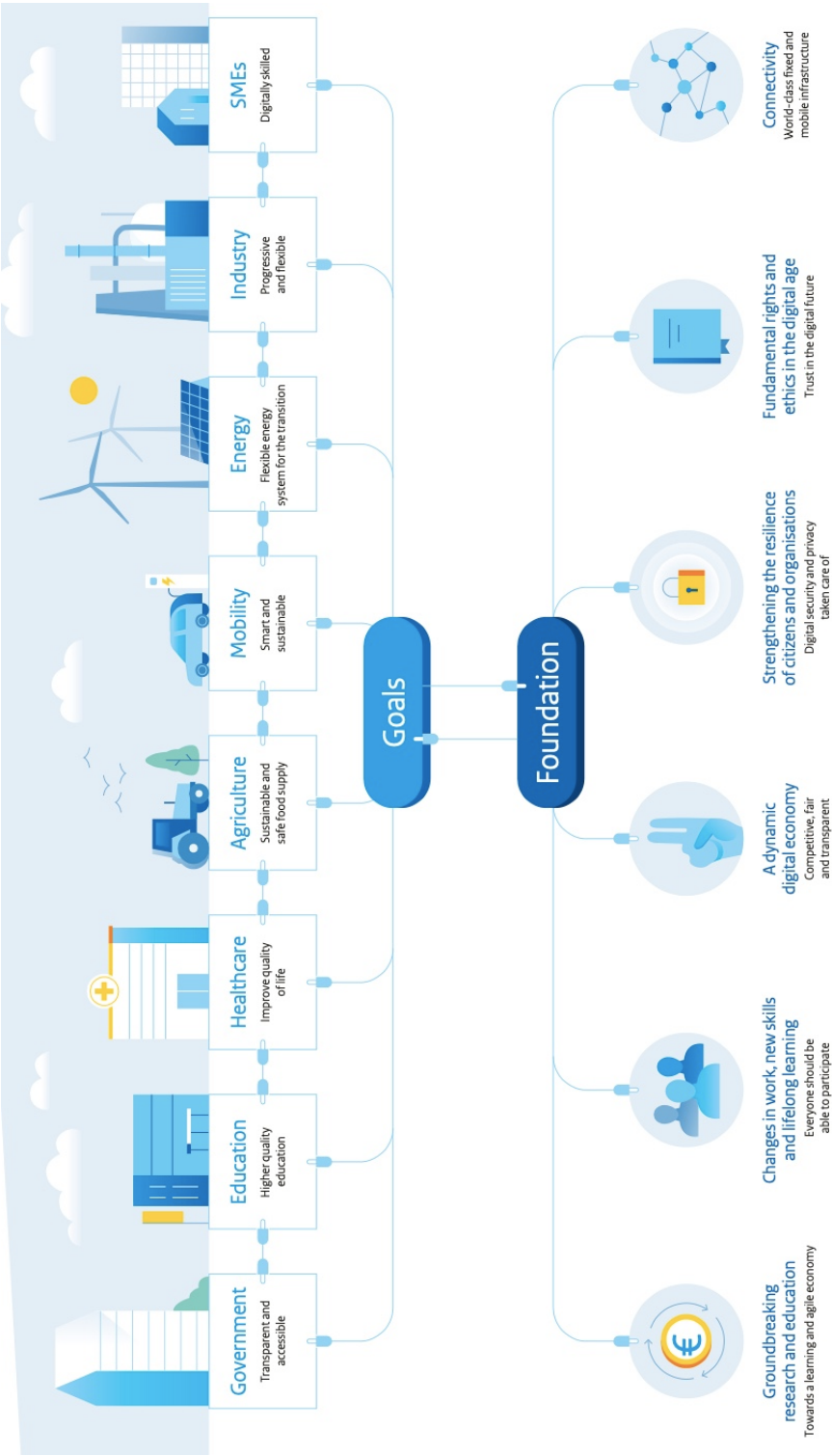
Anexo 4

População total de Amesterdão desde 2009 até 2022



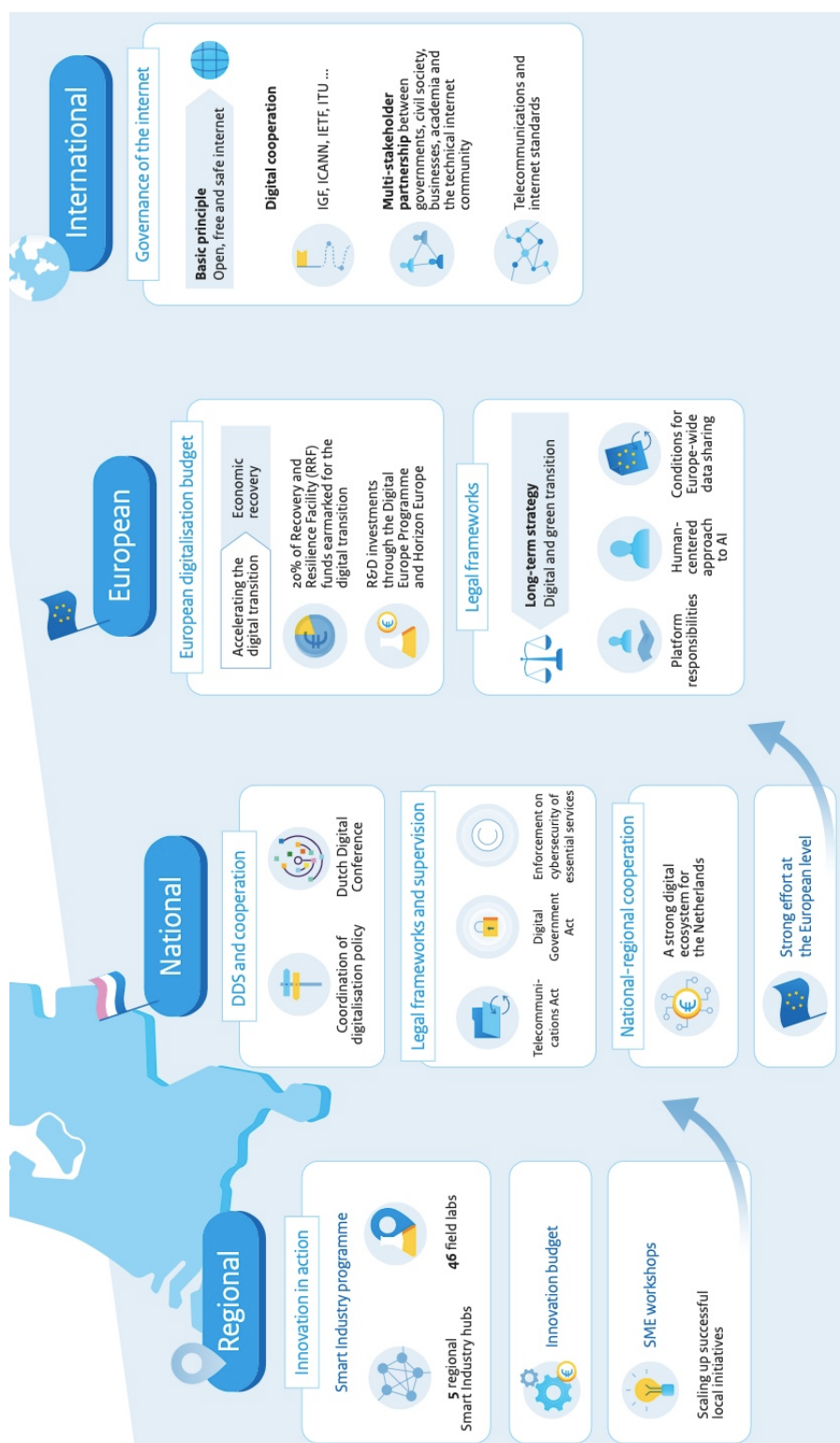
Fonte: Statista.

Estratégia Digital Holandesa



Fonte: The Dutch Digital Strategy.

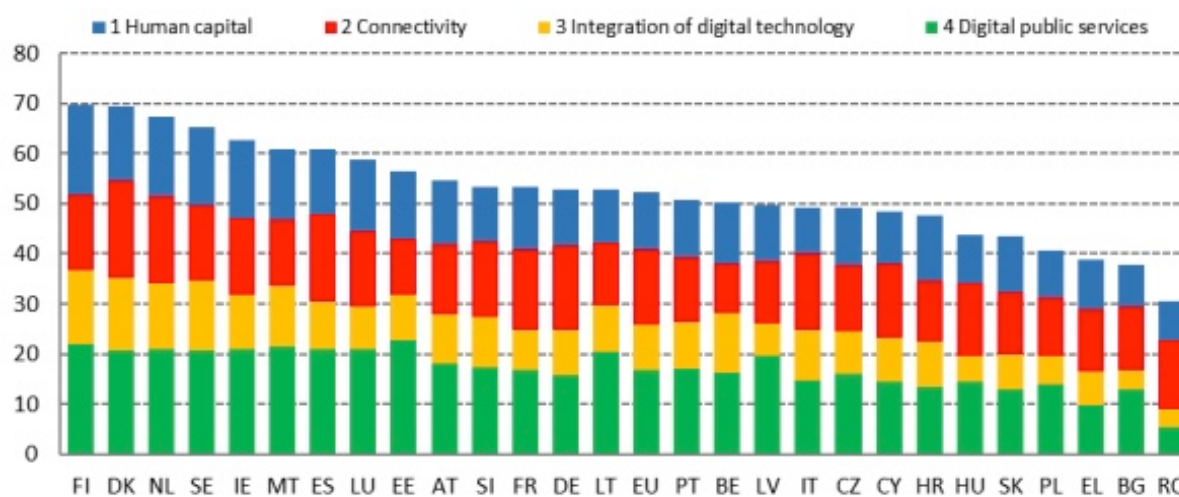
Níveis operacionais definidos pelos Países Baixos



Fonte: The Dutch Digital Strategy.

Anexo 7

Economia Digital e Índice da Sociedade, 2022



Fonte: DESI 2022, Comissão Europeia.

Anexo 8

Sistema de Vigilância Biométrica



Fonte: Parlamento Europeu.