Análise de ciberestratégias e ciberética na segurança nacional: Estados Unidos, Rússia e Portugal

Versão melhorada e corrigida após defesa pública

Catarina Miguel Barreto

Dissertação de Mestrado em Gestão e Curadoria da Informação

Outubro de 2019

Orientadora: Professora Doutora Paula Ochôa

Coorientador: Professor Doutor Roberto Henriques

AGRADECIMENTOS

Se existe alguém que marcou a minha vida académica, essa pessoa é a Professora Paula. Tenho a certeza que sem a sua orientação, disponibilidade, energia e força dada ao longo do último ano este trabalho nunca teria chegado a bom porto e por isso devo-lhe o meu maior agradecimento; ainda assim, reduzir a sua influência no meu percurso apenas a esta fase seria injusto. Enquanto docente e coordenadora do mestrado, a Professora Paula ouviu as minhas dúvidas, opiniões e inseguranças académicas e profissionais e nem uma única vez falhou em me dar uma palavra. Muitas vezes incentivou-me a analisar as situações de outro prisma, outras vezes levou-me a confiar mais em mim e no meu trabalho, e outras quantas (muitas na verdade) foi direta e prática na resolução dos problemas. É de louvar a sua dedicação e esforço para chegar aos interesses académicos dos seus alunos e a ela devo a oportunidade de explorar uma especialização de mestrado não tão óbvia à partida. Caso isso não tivesse acontecido, provavelmente hoje não me sentiria tão realizada profissionalmente como me sinto agora. Do fundo do coração, obrigada Professora.

Ao resto do corpo docente do mestrado, em especial ao Professor Roberto, o meu agradecimento por todos os conhecimentos e competências que me passaram ao longo destes dois anos.

RESUMO

A presente dissertação pretende refletir sobre as limitações éticas no possível comprometimento dos direitos humanos em prol da segurança nacional, contribuindo para a consciencialização das principais questões envolvidas, esclarecendo conceitos e revelando diferenças e semelhanças no que diz respeito a valores, orientações e práticas de ciberguerra, ciberestratégias e ciberética em três zonas geográficas (Estados Unidos da América, Rússia e Portugal) através de uma metodologia comparativa.

Para tal foi realizado um levantamento de informação acerca das características que distinguem a ciberguerra do conflito tradicional e de que forma a ética pode impor restrições nas estratégias e atuação dos estados.

Declarada como um direito humano, a privacidade diz respeito à reserva de informações de índole pessoal e, num mundo digital minado por dispositivos de vigilância massiva, ocupa um lugar de destaque nesta investigação pelo seu carácter atual.

Foram identificadas as seguintes características: a crescente dependência económica dos sistemas de informação; o setor privado de infraestruturas críticas como o alvo principal de ataques; o alargamento dos incidentes de segurança de informação a pessoas singulares; o surgimento de novas formas de ataque e estratégias com novos tipos de armas; o aumento de utilização de *hackers*, éticos e não éticos, ao serviço do sector público e privado; e a inexistência de documentos normativos nacionais que definam os limites éticos no tratamento da informação civil. Constatou-se ainda que que nenhum estado declarou ciberguerra a outro, e por isso é controverso afirmar que a ciberguerra já começou, mas é notória a atual tensão internacional nomeadamente entre os EUA e a Rússia.

Palavras-chave: Ciberestratégias; Ciberética; Privacidade; Segurança Nacional; Estados Unidos da América; Rússia; Portugal.

ABSTRACT

This dissertation aims to be a reflection on ethical limitations in the possible compromise of human rights for the sake of national security, contributing to the awareness of the main issues involved, clarifying concepts and revealing differences and similarities regarding values, guidelines and practices of cyberwar, cyberstrategies and cyberethics in three geographical areas (United States of America, Russia and Portugal) through a comparative methodology.

For this, a research was carried out to understand which characteristics distinguish cyberwar from traditional conflict and on how ethics can impose restrictions on strategies and actions of the states.

Declared as an human right, privacy is the discretion of personal information and, in a digital world overmined by mass surveillance devices, occupies a prominent relevance in this investigation for being an ongoing matter.

The following characteristics were identified: increasing economic dependence on information systems; the private sector of critical infrastructure as the primary target of attacks; the extension of information security incidents to individuals; the emergence of new forms of attack and strategies with new types of weapons; the increased use of hackers, ethical and unethical, to serve the public and private sector; and the absence of national normative documents that define ethical limits in the treatment of civil information. It was also noted that no state has declared cyberwar to another and for that reason it is controversial to say that cyberwar has already begun, but is notorious the current international tension, specially between the US and Russia.

Keywords: Cyberstrategies; Cyberethics; Privacy; National Security; United States of America; Russia; Portugal.

ENQUADRAMENTO

Graças à tendência da transformação digital das organizações, a interdisciplinaridade característica da Ciência da Informação tem vindo a ganhar particular visibilidade e merece ser devidamente explorada. Ajustando-se à necessidade de profissionais com competências em diferentes domínios, surge o *Mestrado em Gestão e Curadoria da Informação* como o primeiro curso superior em Portugal que oferece duas abordagens interdisciplinares face à governança de informação, tendo em conta o contexto organizacional.

Retrocedendo até 2012, no momento da escolha do curso superior a seguir, os meus interesses de formação eram bastante variados. Felizmente, por sugestão dos meus pais, tinha frequentado o ensino secundário em Ciências e Tecnologias, o que me concedeu mais oportunidades de formações académicas às quais me podia candidatar. Tinha curiosidade pela Saúde, Direito e Psicologia e encontrei no plano de estudos da Licenciatura em Ciências Forenses e Criminais todas estas matérias. Esta licenciatura culminava quase todas as minhas áreas de interesse e permitir-me-ia ter uma profissão interdisciplinar como sempre quis, no entanto, por motivos de força maior, não foi possível candidatar-me a este ciclo de estudos. Optei por apostar noutra grande paixão que tinha: as Artes do Espetáculo. Passei os seguintes três anos a estudar diferentes expressões de arte, maioritariamente cinema e teatro, onde desenvolvi a minha criatividade e, principalmente, o meu sentido crítico. Foi também durante estes anos que aprendi que o percurso profissional pode e deverá (se assim o quisermos) ser adaptável, flexível e plástico às nossas ambições e ao ambiente que nos rodeia. Atendendo às necessidades do mercado, optei estrategicamente por apresentar uma candidatura espontânea a uma produtora de televisão para a realização do meu estágio curricular, o qual foi aceite, e onde tive a oportunidade de trabalhar após a conclusão da licenciatura. Ainda que tenha tido uma experiência profissional muito satisfatória, no verão de 2016, voltei a refletir sobre a necessidade de me adaptar à nova demanda profissional, desta vez definida por especialistas com competências digitais. Sensivelmente na mesma altura, aceitei o desafio de me juntar a uma equipa, enquanto responsável por comunicação digital e vendas, no desenvolvimento de um produto

inovador no sector do turismo, e embora tenha aprendido autodidaticamente diversas matérias dentro da esfera do marketing digital, sentia necessidade de uma formação mais sólida, de alto nível e interdisciplinar que me permitisse ajustar, moldar e conciliar com os meus diferentes interesses e as variáveis lacunas do mercado. O Mestrado em Gestão e Curadoria da Informação veio dar resposta ao que procurava, não só por oferecer uma componente curricular bastante ampla e de acordo com a perspetiva de organizações públicas e privadas (fruto da parceria entre as duas faculdades), mas principalmente pela capacidade de adaptabilidade aos interesses individuais de cada aluno e a proximidade entre professores e alunos, sendo um dos maiores pontos positivos do mestrado.

Por si só, a Ciência da Informação é um mundo de interesses, possibilidades, e interdisciplinaridade. Quem se dedica ao estudo desta área tem a consciência que o petróleo da atualidade são os dados, a gasolina é a informação e o conhecimento permite-nos descobrir novos caminhos e desenvolver novas estratégias, mais eficazes e eficientes, para evitar obstáculos. A focalização específica nesta área surge naturalmente desde o primeiro semestre ao verificar que, para além da sua característica transversalidade a outros assuntos, a Ciência da Informação contém em si diferentes subtemas, como a segurança e a ética da informação. Estes são dois temas que ao longo dos últimos três anos têm despertado a minha curiosidade e, por essa razão, é-me particularmente relevante, porém, estas subáreas foram também escolhidas por serem temas atuais e a sua discussão não mostra ser finita no presente momento. Admitindo que a rapidez com que evoluiu a tecnologia não é a mesma com que evoluiu a discussão ética da sua utilização, interessa-me particularmente compreender o comportamento das organizações, sejam elas públicas ou privadas, perante situações que sobreponham valores éticos e morais do uso da Informação e que, direta ou indiretamente, afetem indivíduos exteriores à organização. Sendo este um mestrado orientado para o futuro e tendo em conta os meus interesses em matérias de Ciência da Informação, Direito e Relações Internacionais, examinar as políticas e estratégias de segurança da informação e as implicações do envolvimento de sistemas computacionais na privacidade pareceu-me uma escolha de investigação adequada, ainda que seja um desafio com um nível de complexidade e exigência considerável.

TABELA DE CONTEÚDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ANEXO

SIGLAS

SIGLA	NOME
(ISC)²	*International Information System Security Certification Consortium*
CD	*Compact Disk*
CERT	*Community Emergency Response Team*
CIA	*Central Intelligence Agency*
CNA	*Computer Network Attack*
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
COPPA	*Children's Online Privacy Protection Act*
CSIRT	*Computer Security Incident Response Team*
DHS	*Department of Homeland Security*
DIH	Direito Humanitário Internacional
DNS	*Domain Name System*
DOD	*Department of Defense*
DoS	*Denial of Service*

DUDH Declaração Universal dos Direitos Humanos

EPCA *Electronic Communications Privacy Act*

EUA Estados Unidos da América

FASPSI *Federal'noe Agentstvo Pravitelstvennoi Svyazi I Informatsii* (PT, tradução livre: Agência Federal de Comunicação de Governo e Informação)

FBI *Federal Bureau of Investigation*

FISA *Foreign Intelligence Surveillance Act*

FOIA *Freedom of Information Act*

FSB *Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* (PT, tradução livre: Serviço Federal de Segurança da Federação Russa)

FSO *Federalnaya Sluzhba Okhrany* (PT, tradução livre: Serviço Federal de Proteção)

GNR Guarda Nacional Republicana

GNS Gabinete Nacional de Segurança

HUMINT *Human Intelligence*

IA Inteligência Artificial

IAEDN Instituto de Altos Estudos da Defesa Nacional

IDN Instituto da Defesa Nacional

ISAC *Information Sharing and Analysis Center*

KGB *Komitet Gosudarstvennoy Bezopasnosti (*PT, tradução livre: Comité para a Segurança do Estado)

NATO *North Atlantic Treaty Organization*

NATO CCD COE *North Atlantic Treaty Organization - Cooperative Cyber Defence Centre of Excellence*

NSA *National Security Agency*

OECD *Organization for Economic Co-operation and Development*

ONU Organização das Nações Unidas

OPCL *Office of Privacy and Civil Liberties*

OSCE Organização para a Segurança e Cooperação na Europa

PIDCP Pacto Internacional Sobre os Direitos Civis e Políticos

PSP Polícia Segurança Pública

RGPD Regulamento Geral de Proteção dos Dados

SIED Serviço de Informações Estratégicas de Defesa

SIRP Sistema de Informações da República Portuguesa

SIS Serviço de Informações de Segurança

SORM *System of Operational-Investigatory Measures*

SVR Sluzhba Vneshney Razvedki (PT, tradução livre: Serviço de Inteligência Estrangeira)

TI Tecnologias de Informação

UE União Europeia

UNESCO *United Nations Educational, Scientific and Cultural Organization*

URSS União das Repúblicas Socialistas Soviéticas

Por norma foram utilizadas as siglas na língua em que eram mais conhecidas em Portugal.

ORIENTAÇÃO PARA A CONSULTA DE NOTAS DE RODAPÉ E BIBLIOGRAFIA

1. Os artigos, trabalhos académicos e livros (em suporte físico ou digital) foram na sua maioria referenciados na Bibliografia. Os documentos legislativos e normativos, bem como as notícias e *websites* que suportaram o contexto foram referidos em Nota de Rodapé.
2. A menos que indicado em contrário, todos as hiperligações que facilitam o acesso do leitor à informação utilizada como fonte (tanto na Bibliografia como nas Notas de Rodapé) estavam ativos a 04 de Junho de 2019.

I. INTRODUÇÃO

Com o desenvolvimento de novas tecnologias e a crescente acessibilidade às mesmas, grande parte do conflito internacional migrou do espaço físico para o virtual. Por ser um território partilhado por todos e ao mesmo tempo não dominado por ninguém, o ciberespaço, que podemos considerar como sendo uma extensão da sociedade moderna, tornou-se o campo de batalha preferido dos atacantes pela falta de imposição de fronteiras concretas, sejam elas físicas ou legislativas (HUGHES & COLARIK, 2017). Assim, os Estados interiorizaram a importância do desenho de planos de ação que definissem uma Estratégia Nacional de Segurança do Ciberespaço clara e sobretudo eficaz na defesa nacional.

As estratégias aplicadas ao ciberespaço [1] são particulares a cada país mas frequentemente envolvem a criação de uma estrutura de coordenação político-estratégica focada neste tema e a capacitação dos organismos públicos na deteção, reação e gestão de ciberincidentes[2], o que se traduz num grande investimento em infraestruturas e formação defensiva como preventiva e reativa (VALERIANO, JENSEN, & MANESS, 2008). Os autores acrescentam referindo que as ciberestratégias podem ser entendidas como uma "variante moderna de diplomacia coerciva" que poderá contemplar o uso da força, de uma forma controlada e discreta, para triunfar sobre os seus inimigos. [3] Desenhar e implementar uma ciberestratégia não significa necessariamente substituir outros instrumentos de guerra tradicionais mas sim amplificar e maximizar o poder dos recursos disponíveis.

De acordo com MORAG (2018), a segurança nacional poderá ser funcionalmente caracterizada em três domínios: políticas direcionadas à mitigação de ameaças à estabilidade social e económica; políticas direcionadas à gestão de consequências de

[1] De agora em diante *ciberestratégias*.

[2] Para mais informações consultar a apresentação do CNCS. Fonte: <https://academiamilitar.pt/images/10_SIMPOSIO_INTERNACIONAL/Apresentacoes/1.Estrat-Seg-Ciberespao_CNCS.pdf>.

[3] Os autores baseiam-se na obra de Lévy (2008), contudo, não foi possível encontrar a referência bibliográfica exata.

atos de terrorismo, desastres naturais e/ou emergências de saúde pública; e, por fim, políticas direcionadas a reforçar as medidas de segurança. Adicionalmente à proteção de infraestruturas críticas e reforço da segurança de fronteiras, a cibersegurança insere-se no último domínio. O autor acrescenta que, para o sucesso, estas àreas requerem a partilha de informação, bem como a cooperação interna ou externa de agências e interação com o público.

Após evidentes disrupções tecnológicas, torna-se necessário a adaptação e atualização das políticas e ciberestratégias nacionais. Embora a maturidade do debate tenha vindo a aumentar nos últimos anos, nem sempre as implicações éticas são ponderadas durante a definição desses planos de ação. A reflexão sobre as escolhas e hábitos socialmente definidos no âmbito da produção, utilização e armazenamento da informação dá-se o nome de ética de informação. A ética da informação lida com diferentes questões particulares, tais a ética informacional e a ciberética. De acordo com Capurro, ciberética é uma ramificação muito específica da ética da informação, focada na internet.[4] Os códigos de ética pretendem limitar as práticas tecnológicas e, no âmbito da computação, existem vários que definem que atividades são consideradas antiéticas e inaceitáveis – seguem alguns exemplos[5]:

- Comprometer a privacidade de outros
- Obter acesso não autorizado a recursos disponíveis na internet
- Utilizar dados de outros sem o seu consentimento ou para fins diferentes para os quais foram recolhidos
- Usar o computador como meio para prejudicar outros

Para os profissionais de segurança da informação existe uma entidade certificadora, a (ISC)[2], dedicada a definir cânones para o exercício das suas funções, sendo que o primeiro é proteger a sociedade, o bem comum e assegurar a confiança pública.[6]

[4] Entrevista a Rafael Capurro em 2014 por Rahman Marefat e Mahmood Sangari. Fonte: <http://www.capurro.de/marefat.html>.

[5] Fontes: <https://tools.ietf.org/html/rfc1087>; <https://epic.org/privacy/consumer/code_fair_info.html>; e < http://cpsr.org/issues/ethics/cei/>.

[6] Fonte: <https://www.isc2.org/ethics>.

A ciberguerra[7], quando comparada à guerra tradicional, poderá causar danos igualmente irreversíveis às estruturas vitais da sociedade, contudo as suas dimensões são mais dificilmente mensuráveis tendo em conta que os meios e formas de ataque são imprevistos e muitas vezes repentinos. Nesse sentido, e em particular as organizações militares e governamentais, que ocupam um papel decisivo no desenrolar da ciberguerra pela tecnologia e conhecimento que detêm, têm vindo a apostar cada vez mais na ciberdefesa ativa e passiva dos seus territórios virtuais – o que poderá comprometer os direitos humanos, nomeadamente a privacidade dos indivíduos. O ciberespaço passou a ser figurativo de novo poder - exemplificado pelo desejo dos governos em regularem e controlarem o seu espaço virtual afim de também terem permissão de recusarem a entrada dos outros no seu território cibernético - e de potencial lucro para empresas que oferecem serviços de gestão virtual. A par, a transformação digital e o incentivo do uso do mundo virtual influenciaram diretamente a sociedade, particularmente na partilha e dependência da informação no quotidiano. Em seguida é apresentada uma sistematização da sociedade moderna em rede bem como as forças envolvidas nesta dinâmica (NUNES, 2016) (PASSOS, 2017):

Figura 1 - Sistema de sistemas no ciberespaço (Grossman-Vermas, 2004 cit. Nunes, 2016, p.53)

[7] Ao longo da investigação foi detetada a existência de dois termos em inglês para descrever o fenómeno em estudo: *cyberwar* e *cyberwarfare*. Santos, Bessa & Pimentel (2008, p.99) sugerem uma tradução portuguesa para *warfare* (Aparelho de Guerra), contudo, para efeitos desta dissertação - e considerando que não foi encontrado um critério que distinga a utilização dos dois termos em inglês, parecendo significar exatamente o mesmo, *ciberguerra* foi o conceito adotado correspondente para a língua portuguesa.

Este sistema conectado representa um aumento de oportunidades de defesa de estrutura, interoperabilidade de sistemas, memória pessoal, histórica e social, mas também, proporcionalmente, uma multiplicidade de ameaças de invasão, roubo e perda.

É urgente discutir e regulamentar o ciberespaço na procura da harmonização nacional e internacional das atividades virtuais. A criminalização acaba por ser o ponto central do debate, existindo claramente uma tentativa de estabelecer, ao longo dos últimos anos, o que é *errado* e *certo*, *proibido* e *permitido*. A legislação destina-se à gestão da sociedade e, embora a organização administrativa de um país tenha que estar alinhada às mesmas regras, por vezes, excecionalmente e justificadamente, poderão transcender alguns contornos legislativos visando a missão suprema de proteção nacional. Nestas situações, estabelecer diretrizes éticas, que dependem de valores, é uma tarefa extremamente difícil, principalmente tendo em conta que o *cibercrime*, a *ciberguerra* e a *ciberprivacidade* ainda são tópicos em construção e definição. Para além disso, tudo o que é ligado ao espaço virtual é de todos e de ninguém, o que significa que a concordância ciberética é extremamente difícil de alcançar.

Com o objetivo de estudar de que forma os desenvolvimentos das tecnologias de informação poderão gerir e potenciar o conflito virtual entre países, tendo em conta a dependência da sociedade moderna da informação, bem como as implicações na ciberprivacidade, limitei a minha análise comparativa a três países possivelmente mais interessantes tendo em conta as suas diferenças geográficas, políticas e organizacionais: Estados Unidos da América (EUA); Rússia e Portugal.

Ainda que os EUA sejam um dos países mais investigados nesta matéria, principalmente após a revelação mediática dos complexos sistemas de vigilância americanos por Edward Snowden em 2013, faz sentido incluí-los na análise tendo em conta que são um dos países mais interessados nesta matéria e que investem mais tecnologia no ciberespaço.

A Rússia, por outro lado, é um país que desperta curiosidade por todo o secretismo mas evidente vontade em ocupar uma posição marcante no ciberespaço. Tendo em conta o historial de conflitos entre as duas regiões, e por ambas investirem fortemente no desenvolvimento tecnológico, são potencialmente interessantes de analisar.

Atendendo que em Maio de 2018 entrou em vigor o Regulamento Geral de Proteção de Dados (RGPD), que contempla a privacidade e proteção de dados pessoais de indivíduos do espaço económico europeu, torna-se pertinente incluir a União Europeia (UE) nesta análise pela preocupação que demonstram com esta medida. Contudo, considerando que a União Europeia é o resultado de uma parceria político-económica de alguns países europeus[8], que embora partilhem um mecanismo de gestão de crises, nomeadamente no âmbito civil, cada países-membro da União Europeia é regidos de forma autónoma e independente, seria muito difícil descobrir se existe uma relação entre o padrão de ação dos países de estudo, em situação de ciberguerra, tendo em conta que partilhavam apenas parte das diretrizes de governança. A escolha de Portugal surgiu estrategicamente de forma a limitar e especializar o estudo por ser um país com uma crescente preocupação no tema, representada por palestras e aumento da oferta académica na área, e por ser uma realidade mais próxima.

Posto isto, é relevante mencionar que os Estados Unidos são reconhecidos como o país mais debatido quando falamos de ciberguerra e, por isso, existem vários trabalhos académicos e militares sobre a atividade norte-americana em ciberconflitos[9], ao contrário dos outros dois países da amostra. Em geral, os trabalhos neste âmbito procuram principalmente definir o posicionamento dos países de acordo com a sua a capacidade tecnológica e prever as possíveis consequências a nível internacional, contudo, o comprometimento de direitos humanos, como a privacidade dos cidadãos, e as implicações éticas da utilização da informação para fins de proteção nacional, são assuntos consideravelmente menos falados, o que se transformou numa oportunidade interessante de contribuição para este tema. Existem alguns artigos militares e dissertações académicas em Português acerca do posicionamento de Portugal relativamente à transformação e dependência tecnológica, ética militar, privacidade, cibercrime e até mesmo ciberguerra[10], mas em Portugal o tema é explorado de uma perspetiva distante (talvez porque seja difícil para Portugal rever-se nesta realidade,

[8] Ainda que façam parte desta aliança, os países-membro da União Europeia são regidos de forma autónoma e independente uns dos outros.

[9] São alguns exemplos: (LAWSON & MIDDLETON, 2019), (CLAPPER, ROGERS, COMMANDER U. S. N., & COMMANDER U. C., 2017) e (INKSTER, 2016).

[10] São alguns exemplos: (PASSOS, 2017), (SANTOS, 2017) e (GONÇALVES, 2016).

tanto como atacado como atacante) e quase sempre numa perspetiva de comunicar boas práticas de governação da informação, mostrar a conformidade com as políticas europeias ou esclarecer o panorama legislativo do ciberespaço, em particular da Lei do Cibercrime. Em alguns trabalhos, são mencionadas e investigadas as repercussões dos cibereventos nas relações internacionais, tal como em GONÇALVES (2016), mas habitualmente o assunto é tratado com uma subdivisão de um tópico mais abrangente.

De acordo com a informação disponível, verifica-se que o número de estudos relativos à abordagem da Rússia à ciberguerra é consideravelmente baixo[11], quando comparado aos EUA. Para além disso, para os russos o *cyber* é compreendido como um mecanismo auxiliar que permite ao estado dominar a esfera informacional, sendo essa razão pela qual o termo ciberguerra não é frequentemente utilizado por estes (CONNELL & VOGLER, 2017), o que poderá representar um obstáculo adicional para a análise comparativa. Não foi encontrado nenhum estudo dedicado concretamente às questões de privacidade e ética da informação na Rússia em contexto de proteção nacional. Grande parte da informação que o governo russo disponibiliza e que diz respeito à legislatura e estrutura governamental está escrita em alfabeto cirílico, dificultando a interpretação do conteúdo mesmo que recorrendo a *softwares* de tradução. Contudo, por ser um dos principais adversários dos EUA, a Rússia é um país com um enorme potencial em ser estudado nesta matéria, principalmente após ter conferido asilo político a Edward Snowden, acusado pelo Governo dos Estados Unidos de roubar propriedade do governo e divulgar publicamente informação confidencial relacionada com o sistema de vigilância da NSA (National Security Agency).

Frequentemente são utilizados os ciberataques à Estónia, Geórgia e Irão como exemplificativos de atos de ciberguerra e alguns autores concentraram as suas investigações na atribuição desses ataques à Rússia (DEIBERT, ROHOZINSKI, & CRETE-NIISHIHATA, 2012) ou aos EUA (FARWELL & ROHOZINSKI, 2011).

Durante a fase de recolha de informação, não foi encontrado nenhum estudo, nacional ou internacional, que compare estes três países nestes parâmetros (ciberestratégias, ciberética e privacidade na segurança nacional), embora tenham sido encontrados textos dedicados aos temas de forma individual e, por vezes, agrupando

[11] São alguns exemplos: (CONNELL & VOGLER, 2017) e (GADY & AUSTIN, 2010).

um dos temas e respetivos exemplos dos três países no mesmo documento.[12] Foi verificada a existência considerável de artigos de opinião e notícias que debatem as atuações dos países para defesa nacional, nomeadamente no possível comprometimento da privacidade nos países em análise (ainda que de uma forma individual).[13]

a) Objetivos

Com este estudo, pretende-se responder à questão de investigação - de que forma a segurança nacional pode comprometer os direitos humanos e se a ciberética pode efetivamente moderar as ciberoperações estatais?

Pretende-se igualmente refletir sobre as ciberestratégias e ciberética na segurança nacional num mundo cada vez mais digital; conhecer os diferentes sistemas, leis, políticas e estratégias de segurança nacional de três áreas globais (Estados Unidos, Rússia e Portugal) e, por fim, explorar em particular a forma como a segurança nacional pode comprometer os direitos humanos (em particular da privacidade). Este trabalho pretende contribuir para a consciencialização dos temas acima apontadas, esclarecendo conceitos e revelando diferenças e semelhanças no que diz respeito a valores e orientações dessas três zonas globais.

b) Metodologia

No que toca à metodologia, propõe-se uma análise prática e comparativa de políticas e ciberestratégias de segurança de informação e defesa nacional dos Estados Unidos, Rússia e Portugal, de forma a concluir quais as implicações na privacidade dos

[12] Por exemplo, o documento "*Privacy, Data Protection and Cybersecurity Law Review"* (RAUL, 2017) é resultado de uma compilação de textos de diferentes autores que esclarecem como as questões de privacidade, proteção de dados e cibersegurança é aplicada nos seus países. Neste documento estão incluídos vários países, entre os quais EUA, Rússia e Portugal, e por essa razão foi uma fonte frequentemente utilizada.

[13] Em 2017, a *Central Intelligence Agency* (CIA) revelou novas regras para a recolha de dados de cidadãos norte-americanos que pretendiam proteger a privacidade e os direitos civis. Por outro lado, enquanto candidato à presidência Donald Trump já tinha manisfestado a favor de um reforço de vigilância nomeadamente em certas mesquitas. Fonte: < https://www.dinheirovivo.pt/economia/novas-regras-cia/>.

cidadãos de cada um dos países, recorrendo a um raciocínio indutivo. O recurso à comparação como metodologia de trabalho é uma prática comum em vários campos, nomeadamente em estudos sociais, contribuindo para o seu desenvolvimento enquanto disciplinas científicas (LOR, 2011). Ainda que orientada para o estudo da Gestão da Informação digital[14] em situações de crise nacional, esta investigação só poderia ser feita abordando vários temas das Ciências Sociais, tais como a Ciência Política, o Direito e as Relações internacionais. Conforme Paden (2001, p. 195) e Linãn (2008), a comparação é uma questão de classificação e uma estratégia analítica para fins não só descritivos, mas também explicativos, tornando-se numa ferramenta de entendimento (GOMES & DA CRUZ, 2016) - sendo esse o objetivo dominante desta dissertação.

A metodologia comparativa poderá ramificar-se em quantitativa ou qualitativa, de acordo com determinadas características (Tabela 1), contudo, segundo Hantrais (2009, p. 59 e p. 103-108), a bifurcação quantitativo *versus* qualitativo poderá ser extremista e impraticável para determinadas situações. No caso particular desta análise foi adotada uma abordagem metodológica pluralista[15], com uma forte predominância *qualitativa*. Ainda que seja eu seja uma cidadã portuguesa e um dos países em estudo seja Portugal, a minha observação e análise é feita completamente do exterior porque não possuo nenhum tipo de relação com as organizações estudadas. Para além disso, este acaba por ser um estudo empírico pois baseia-se na observação, ainda que sejam consideradas para a análise regras e normas éticas, resultando numa metodologia mista.

[14] Mais precisamente do seu tratatamento, que engloba as sub-atividades de recolha, análise e armazenamento da informação.

[15] Marcada pela utilização de uma metodologia com características quantitativas e qualitativas. As características metodológicas utilizadas nesta investigação estão selecionadas a verde-claro na Tabela 1.

CARACTERÍSTICA	QUANTITATIVA	QUALITATIVA
METATEORIA	Positivista, Pós-positivista	Interpretativista
NATUREZA DA REALIDADE	Singular, estável, independente do observador; realidade externa	Multifacetada, determinada culturalmente, socialmente construída; realidade holística
RELAÇÃO DO INVESTIGADOR COM O QUE É INVESTIGADO	Externa, observação pelo exterior; num cenário artificial	No ambiente em estudo, observação do interior; num cenário real
RELAÇÃO COM O FENÓMENO SOCIAL	Neutra Empírica	Comprometida Normativa
OBJETIVO DA INVESTIGAÇÃO	Nomotético, teste de hipóteses; generalização	Ideográfica, estabelecimento de hipóteses; contextualização
ESTRATÉGIAS	Estruturada, variáveis orientadas pela teoria identificadas previamente; controlo; operacionalização e medição	Teoria não estruturada, aberta, desenvolvida durante a pesquisa; conceitos ricos em significado
MÉTODOS COMUNS	Experimentações, questionários	Observação dos participantes, estudos de caso
CRITÉRIOS DE ANÁLISE DA INVESTIGAÇÃO	Validade e confiabilidade, objetividade	Credibilidade, transferibilidade, confiabilidade, autenticidade

Tabela 1 - Método comparativo qualitativo e quantitativo (LOR, 2011) aplicado a esta análise

Numa primeira abordagem, pretende-se investigar individualmente e registar os aspetos a comparar (*níveis de análise*), nomeadamente o contexto histórico, geográfico, legislativo e organizacional de cada país. Seguidamente, pretende-se identificar diretamente as variáveis (*unidades de análise*) tendo em conta os níveis de análise explorados, com a ajuda de uma matriz de dados que auxiliará a identificação de semelhanças e diferenças (LOR, 2011).[16] A terceira etapa deste método comparativo, foca-se na descrição e juízo dos resultados obtidos pela comparação, orientada quando possível por exemplos práticos (*estudos de caso*), procurando fundamentar argumentos que os justifiquem.

[16] Esta matriz estará disponível em Anexo.

c) Estrutura

Após uma contextualização e introdução à transformação digital, o ciberespaço é definido como o novo campo de batalha. Em seguida, é introduzida a ética da informação, aplicada a este contexto, como uma das formas de regulamentação e restrição das práticas de informação.

Segue-se a revisão de literatura dedicada essencialmente à fragmentação do tema da ciberguerra e descrição da forma como os métodos preventivos de vigilância massiva podem afetar o exercício do direito à privacidade.

As três primeiras seções do antepenúltimo capítulo dedicam-se a compilar informação relativamente ao *contexto histórico, geográfico e político*, à *segurança nacional*, à *cooperação internacional* e à *legislação nacional para a privacidade e proteção dos dados* de cada um dos países. Na última seção são comparadas as ciberestratégias dos três países e evidenciados alguns modelos de atuação em circunstâncias associadas a *ciberataques*, *ciberdefesa*, *ciberguerra* e *privacidade*. É também neste momento que é feita a reflexão se a privacidade civil já foi/pode ser posta em causa em prol da segurança nacional e, se afirmativo, se as finalidades para a invasão da privacidade eram de alguma forma válidas (legislativamente e eticamente). Por último, são apresentadas as considerações finais.

II. O CIBERESPAÇO COMO O NOVO CAMPO DE BATALHA

A integração de novas tecnologias nos processos de gestão de informação alterou consideravelmente a dinâmica organizacional de entidades públicas e privadas, relativamente à produção, armazenamento e troca de informação *intra* e *extra* institucional. Com a proliferação dos dados em grande quantidade, velocidade e variedade, comummente apelidados de *big data*, a utilização de Tecnologias de Informação (TI) tornou-se uma necessidade de apoio à tomada de decisão, agora baseada em evidências, recorrendo a sistemas de análise de dados, e a uma escala global. A adaptação a esta nova realidade proporcionou uma melhor sustentabilidade ou, em certos casos, a sobrevivência de algumas organizações, pela sistematização e entendimento dos seus próprios dados, que poderá traduzir-se numa vantagem competitiva face a desafios inesperados. Embora a Gestão de Informação seja um assunto pioneiramente e ainda frequentemente explorado por especialistas interessados no meio empresarial, ao longo dos últimos anos organismos governamentais têm vindo a explorar os benefícios de uma boa governança da informação. Todavia, há que ter em conta que a transformação digital implica uma conduta informacional particular e diferente da que tem sido adotada até aos dias de hoje.

Admitindo que vivemos uma economia baseada no conhecimento, em que a informação passou a ser ativo comercial, a dosagem de confiança e a probabilidade de dependência das organizações nas TI aumentou consideravelmente (GREMBERGEN, 2004). Esta dependência poderá acontecer a dois níveis: tanto porque poderá haver uma desnecessária e volumosa recolha e armazenamento da informação a fim de não se perder nenhum detalhe que possa ser crucial para a tomada de decisão, como porque a excessiva crença e segurança nas TI, facilmente poderá ser posta em causa se existirem vulnerabilidades no sistema.

Embora as consequências dos ataques sejam mais avassaladoras agora, muito devido aos desenvolvimentos tecnológicos e pela confiança depositada nos mesmos, é importante referir que os crimes relacionados com sistemas de informação e comunicação, não é algo particular do século XXI. Ferir pombos correio, interferir com

os sinais de rádio, cortar linhas telefónicas e adulterar informações conscientemente, são também formas de condicionar o funcionamento destas estruturas e provocar danos a diferentes escalas e de variadas formas (CATH, GLORIOSO, & TADDEO, 2016). A perspetiva de uma guerra provocada, focada e alimentada por informação tem sido explorada desde os anos 90, com um particular foco nos Estados Unidos. Para qualquer contexto, não só o militar, entende-se como *guerra da informação* o conjunto de operações de informação que têm como objetivo influenciar, perturbar, corromper ou usurpar estruturas informacionais, afetando assim o processo de tomada de decisões de adversários (U.S. DEPARTMENT OF DEFENSE, 2013). De um ponto vista militar, as ciberoperações acabam por ser uma evolução da guerra eletrónica, usada desde o final da 2º Guerra Mundial, mas adaptada à época contemporânea (RUHMANN, 2013).

O ritmo vertiginoso com que evoluíram as tecnologias de informação na última década possibilitou novas abordagens, acompanhadas de diversas vantagens mas também problemas. Há 20 anos atrás, Dorothy E. Denning, uma investigadora americana especialista em segurança de informação, já tinha evidenciado alguns desses problemas e considerado a possibilidade de nos estarmos a aproximar cada vez mais de uma nova guerra, ainda que em diferentes moldes. O alvo continua a ser a informação, mas o campo de batalha passa a ser o ciberespaço. Tudo o que envolve a governança de um país – economia, alimentação, eletricidade, entre outros – poderá ser comprometido à distância de um *clique*, e às vezes até por jovens ou simples entusiastas dos temas (DENNING, 1998). Por essa razão, a partir dos anos 90, vários países começaram a refletir sobre doutrinas relacionadas com a guerra baseada em sistemas de informação e consequentemente a desenvolver recursos militares de ciberdefesa[17] e ciberataque. Assim, em muitos países, as forças armadas colaboram com serviços de inteligência, que no seu conjunto formam as unidades de guerra de informação, com vista a estarem preparados contra eventualidades (RUHMANN, 2013).

Santos, Bessa & Pimentel (2008) expõem seis princípios de guerra aplicáveis a esse novo campo de batalha:

[17] Passos (2016) citando Ralo (2013) descreve ciberdefesa como "as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco a soberania e a segurança nacional (ciberguerra) e cuja responsabilidade de resposta recai nas Forças Armadas".

MAIOR **OFENSIVA**	O ritmo e a iniciativas das operações, bem como a capacidade de modalidades de ataque às estruturas de um país são significativamente maiores, o que traduz por um aumento do número de oportunidades.
FATOR **SURPRESA**	A facilidade de acesso às estruturas de informação e dependência nas mesmas permite a execução de ataques repentinos, inesperados e dissimulados.
ECONOMIA DE **FORÇAS**	A gestão de conhecimento permite direcionar o esforço nos locais e alturas decisivas.
MARGEM DE **MANOBRA**	O ciberespaço permite uma grande quantidade de opções e liberdade de ações de ataque, oferecendo uma perda reduzida ou inexistente de pessoal e material.
MAIOR **SEGURANÇA**	O controlo de vulnerabilidades dificulta a intervenção e o efeito surpresa do adversário, reduzindo-lhes a liberdade de ataque, e permite que as operações militares sejam o foco.

Tabela 2 - Princípios de Guerra aplicáveis ao ciberespaço, cf. Santos, Bessa e Pimentel (2008)

Segundo a Associação para a Promoção e Desenvolvimento da Sociedade de Informação, entende-se como ciberespaço o espaço virtual criado por redes de computadores onde as pessoas comunicam de diferentes maneiras e se conectam[18]. Em 1993, Al Gore pressagiou que o ciberespaço seria mais do que um novo espaço social. A nova esfera digital traduzir-se-ia num agrupamento de novas oportunidades não só de trabalho e entretenimento, mas também de promoção de educação e aumento da participação política e democracia. Referiu também que as novas formas de comunicação "salvariam vidas" (KOLLOCK & SMITH, 1999). O ponto de vista de Al Gore foi o propulsor para o início do debate desta dissertação. Sem dúvida que, hoje, passado 25 anos, as novas formas de comunicação literalmente salvaram vidas, por exemplo em fornecer assistência médica em situações de catástrofe, mas a que custo? Até que ponto, o atual (ab)uso do ciberespaço coloca em causa a privacidade dos cidadãos, sem o consentimento dos mesmos?

O ciberespaço tornou-se num catalisador e facilitador do crime e da cibervigilância, sendo a sobre-exposição a principal característica negativa. Os crimes passaram a poder ser feitos a partir do outro lado do mundo e tudo o que era preciso era um computador e competências digitais, que podem ser adquiridas no espaço

[18] Definição de ciberespaço, presente no Glossário da Sociedade de Informação, e de acordo com a Associação para a Promoção e Desenvolvimento da Sociedade de Informação. Fonte: <https://apdsi.pt/glossario/c/ciberespaco/>.

virtual. O estímulo de aprendizagem que a nova era digital iria proporcionar e que Al Gore referiu, também poderia significar a disseminação de conhecimento com propósitos maliciosos, todavia, era uma hipótese muito remota para ser refletida na altura, até porque talvez não se tenha calculado que a evolução acontecesse tão rapidamente. Assim, o crime migrou do mundo físico para o virtual e com isso o crime ganhou novas proporções, formas e também uma caracterização e identificação mais difícil dos criminosos. Visto isto, o ataque no ciberespaço, via tecnologias de informação, "dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e comunicação (confidencialidade, integridade e disponibilidade)" - mas não só - denomina-se *ciberataque*[19] [20]. Ainda que se pense à partida que um ciberataque acontece via internet, podemos alargar o espectro de ferramentas a outros tipos de média como CD's, *pendrives*, aplicações ou sistemas de operação distribuídos em intranet, bem como humanos que, deliberadamente ou não, poderão ser veículos dinamizadores do ataque (DIPERT, 2010).[21] Por relação, o crime informático, também apelidado cibercrime ou crime digital, é o ataque delituoso contra um sistema de TI com recurso a computadores e/ou à Internet, mas é muito mais difícil de classificar bem como de identificar, tendo em conta que é um conceito anexado a uma componente legal. Uma vez que não existe um consenso universal, detalhado e uniforme acerca daquilo que estipula um cibercrime, é difícil que a sua definição seja consensual, bem como as suas consequências legais.[22] Mas até que ponto é que um ataque informático autorizado pelo governo, e visando os interesses nacionais, não é por si só um cibercrime também e por essa razão igualmente condenável?

Ainda que não tenham reconhecido que pretendem usar a *web* como um campo de batalha para fins hostis, mas sim como uma estratégia de segurança de informação

[19] Definição de ciberataque, presente na Austrian Cyber Security Strategy. Fonte: <http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50999> , consultada a 06/06/2018.

[20] Definição de ciberespaço e ciberataque, presente no Glossário do Centro Nacional de Cibersegurança, de acordo com diversas fontes. Fontes: <https://www.cncs.gov.pt/recursos/glossario/>.

[21] De acordo com o Memorando "*Joint Terminology for Cyberspace Operations*" (2010). Fonte: <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

[22] O cibercrime é legislado em Portugal pela Lei n.º 109/2009 (Lei do Cibercrime), nos EUA é regulado pelo Network Crime Statutest e na Rússia não foi encontrada nenhuma lei específica a este âmbito.

e resposta aos potenciais ataques, os Estados Unidos consideram o ciberespaço como o quinto domínio das operações militares (ALTMANN & VIDAL, 2013).[23] [24] A defesa é um ato de sobrevivência e por isso aceitável, e de certa forma justificável, contudo, a preparação para defesa contra um hipotético ataque pode fazer com que, à vista de outros países, isso implique que estão "armados" não só para se defenderem, mas também para atacar, visto que a defesa poderá implicar o contra-ataque, o que pode de certo modo suscitar o interesse de inimigos e encorajar à espionagem. Nunca é demais esclarecer que apesar de ser uma dimensão intangível, o ciberespaço está ligado e influencia o mundo real (ALTMANN & VIDAL, 2013), o que poderá elevar os ciberataques a um patamar mais destrutivo do que inicialmente se pensava. De acordo com Passos (2017), os Estados podem empregar ações de ciberdefesa desde que as estratégias utilizadas respeitem os critérios do direito à guerra patentes na Carta das Nações Unidas. O autor acrescenta que a "ciberdefesa ultrapassa […] o limiar da paz e tem como campo de atuação primordial, a ciberguerra".

Quando se fala em ciberataque, é comum imaginar o computador pessoal ou profissional, de torre ou portátil, como sendo o alvo de ataque. Esta associação é coerente porque é um dos alvos favoritos dos atacantes, principalmente hoje em dia em que utilizamos o computador para o armazenamento de diversos tipos de informação pessoal, mas não se restringe a esse formato convencional. Todos os aparelhos que possuam mecanismos de armazenamento e/ou o processamento dos dados virtuais podemos chamar de computador, o que significa que, no nosso dia-a-dia, interagimos com diferentes máquinas, vitais ou não, que registam constantemente a nossa pegada digital (p. e. *pacemakers*, automóveis, *smartphones*, entre outros). Segundo Lévy (p. 44, 1997), o ciberespaço é por si só um computador "hipertextual, disperso, vivo, fervilhante [e] inacabado", "cujo centro está em toda parte e a circunferência em lugar algum" e que está ligado a outros computadores da rede e outros aparelhos de leitura e exibição de informação (SIMÕES, 2009). A *United Nations Educational, Scientific and*

[23] Fonte: <https://www.reuters.com/article/us-usa-defense-cybersecurity/pentagon-to-treat-cyberspace-as-operational-domain-idUSTRE76D5FA20110714>.

[24] Fonte: <http://thehill.com/policy/technology/171531-pentagon-declares-the-internet-a-domain-of-war>.

Cultural Organization (UNESCO) descreve o ciberespaço[25] como sendo algo que envolve pessoas de "todos os países, culturas, linguagens, idades e profissões […] que fornecem e solicitam informação, bem como uma rede global de computadores interconectados pelo meio de infraestruturas de telecomunicações que permitem que a informação seja processada e transmitida digitalmente". De domínio interativo e aberto, o ciberespaço é um espaço de expressão, informação e transação, que fornece uma variedade de propósitos que não estão bem limitados. Identificada essa lacuna, a organização tentou criar uma *framework* universal de normalização e regulamentação do ciberespaço[26] baseada nos seguintes aspetos: *ética* (respeitando valores e princípios jurídicos presentes nos instrumentos internacionais como liberdade de expressão, acesso universal à informação e privacidade); *tecnologicamente neutro* (considerando as diferentes circunstâncias de cada país); *multi-forme* (medidas tecnológicas, jurídicas e educativas) e *universalmente* reconhecido. Da bibliografia consultada, não foi encontrada nenhuma referência a este documento, pelo que é possível que este recurso normativo não seja utilizado pelo menos com a frequência inicialmente esperada.

Para o filósofo e sociólogo francês Lévy, o computador deixou de ser o *centro* e passou a ser o *nó* que interliga a rede universal, e, por isso, influencia a relação das trocas entre a sociedade, cultura e novas tecnologias. Como resultado, e não obstante dos seus benefícios, a existência de uma rede virtual global e aberta dificulta claramente a filtragem dos perigos - perigos esses que se deslocam a uma velocidade quase instantânea quando conectados à *internet* – provenientes e vinculados a determinados computadores. O uso do computador pode resumir-se (mas não se limita) às seguintes formas: (a) *o computador* [de terceiros] *é o alvo de ataque*; (b) *o computador é a arma de ataque*; e, de forma muito comum, (c) *o computador é um acessório* [normalmente com funções de armazenamento de informações].[27]

Quando se reflete sobre um ciberataque, diversos fatores devem ser tidos em conta como o *tipo*, a *técnica*, o *objetivo* a cumprir e as *motivação* do atacante, que por sua vez estão diretamente relacionados com o(s) alvo(s) em questão. Existem vários

[25] Os termos *information superhighways e info sphere* também podem ser utilizados como sinónimo de ciberespaço segundo a UNESCO.

[26] "*The International Dimensions of Cyberspace Law*"

[27] Fonte: <http://www.cybercitizenship.org/crime/crime.html>.

tipos de ataque, como por exemplo a recusa de serviço (DoS – *Denial of Service*) para chantagem (*ransomware*), o envio de mensagens não solicitadas para roubo de informações (*phishing* ou *smishing*), o disfarce do domínio de um *website* para envio de software malicioso[28] (*DNS - Domain Name System*), a cópia e distribuição não autorizada de conteúdo (*pirataria*), entre outros. A um nível mais lato, o *hacking* surge como o termo da esfera do cibercrime que caracteriza genericamente o acesso não autorizado a sistemas computacionais nos quais os direitos de propriedade são claramente violados (WALL, 2005) com vista à obtenção de informações que seriam de outra forma inacessíveis. Um ataque de pirataria, por exemplo, não é dependente da prática de *hacking*, contudo, estes crimes podem correr em simultâneo se a informação a ser copiada se encontrar num sistema restrito a um ou mais utilizadores. De acordo com os objetivos do atacante, a maturidade do crime poderá ser ainda mais elevada podendo existir, para além da cópia, a corrupção, roubo ou eliminação dos dados.

Atualmente existem uma variedade de *técnicas* de ataque (ou metaforicamente *balas*) para invadir e/ou provocar danos nos sistemas de informação e comunicação digitais, na sua maioria sobre a forma de códigos maliciosos (*trojan horses* e *worms*). Estes pretendem tirar vantagem de defeitos, falhas ou vulnerabilidades e causam comportamentos acidentais ou imprevistos no sistema operacional do dispositivo, facilitando o processo de espionagem, cópia, roubo ou destruição dos dados. Em computação, o *trojan horse* inspira-se na lenda da guerra troiana e segue a mesma estratégia. O vírus entra na máquina mascarado como uma aplicação ou ficheiro que não aparenta ser uma ameaça. Muitas vezes, o ficheiro malicioso corre no aparelho durante algum tempo sem que o utilizador se aperceba. Durante esta fase, o *trojan horse* pode estar a recolher informação e/ou a contaminar o smartphone com *worms* – código malicioso que se multiplica e infeta todo o sistema, como se de um "parasita" se tratasse. Com vista a melhores resultados para o criminoso, DELAC, SILIC & KROLO (2011) sublinham igualmente que os ataques costumam ser resultado de uma combinação das inúmeras variantes dos malwares.[29]

[28] Em Inglês *malicious software* é normalmente abreviado para *malware*. Atualmente, esta nomenclatura é reconhecida universalmente.

[29] No âmbito deste mestrado foi efetuada, em conjunto com o colega João Cerdeirinha, uma investigação sobre *Segurança mobile* para a unidade curricular Gestão e Sistemas de Informação.

Como já referido anteriormente, os *objetivos* podem ser inúmeros, desde testar vulnerabilidades, passando pela fraude e extorsão e, em última instância, terrorismo. Opto pelo foco particular na espionagem, por entender ser um dos objetivos mais frequentes em cenário de guerra, seja ela tradicional ou moderna. Esta é uma prática com milhares de anos e já no século IV a.C, no tratado militar *A Arte da Guerra*, a espionagem foi mencionada como sendo uma útil e eficaz estratégia militar, sendo um *meio* para atingir um *fim*, e a sua utilização traria uma probabilidade maior de sucesso considerando que, através da espionagem, era possível descobrir vulnerabilidades do inimigo e prever os seus ataques. Segundo o Serviço de Informações de Segurança (SIS) português[30], a "espionagem não desapareceu, [tornou-se antes] mais complexa e difusa, fruto do aumento da competitividade económica entre as principais potências mundiais e da diversificação, à escala mundial, das ameaças e dos riscos nos planos social, político e militar". O aparecimento de novos meios (como o ciberespaço) e técnicas cada vez mais sofisticadas (como tecnologias de penetração) tornou a espionagem mais eficaz, acelerando a sua prática e frequência. Sabe-se que, em pleno conflito, vigiar o inimigo é fundamental para adaptar a estratégia de guerra, no entanto, contrariamente a essa postura agressiva, e provavelmente muito devido a nenhum dos três países em questão se encontrar em guerra oficial com outro, a espionagem é utilizada como um método preventivo e defensivo. Os países querem ter na sua posse a maior quantidade de informação, o que lhes permite ter um maior conhecimento sobre o inimigo para que possam agir rapidamente em conformidade e eficácia. Contudo, para atingir esse tal conhecimento, é preciso recolher uma quantidade exorbitante de dados que dizem respeito ao estado, incluindo não só a esfera militar como a civil. De certa forma, é compreensível que não façam distinção do grupo a espiar porque, como já referido previamente, existe uma tendência para considerar todos os que pertencem ao país inimigo como sendo da "equipa adversária". O que por vezes não é tão evidente é que a vigilância exaustiva não acontece apenas externamente, entre países, mas também internamente, do estado sobre os seus próprios cidadãos, fruto da desconfiança que todos podem ser inimigos ou espiões de outros países. O fato de gravarmos involuntariamente ou voluntariamente os nossos dados nos computadores, inseridos

[30] Fonte: <https://www.sis.pt/ameacas>.

num sistema interligado, permite a quem tenha habilidades e recursos tecnológicos para tal - onde se pode incluir o estado em si - possa obtê-los de uma forma muito mais simples e imediata caso tenham esse interesse.

A falta de profissionais com competências em cibersegurança mostrou ser uma oportunidade para universidades de todo o mundo. Anteriormente, a cibersegurança era uma subespecialização da Informática, porém, tendo em conta o contexto atual, observa-se a necessidade de alargar a formação a outras áreas, como o Direito e as Relações Internacionais, em cooperação com entidades relacionadas com a defesa nacional, a fim de formar novos profissionais com competências transversais ao que envolve a segurança de informação no ciberespaço. Estas novas formações incluem matérias como Engenharia Social, Direito e Ética na Cibersegurança, Informática Forense, Gestão de Crises no Ciberespaço e *Hacking* Ético. [31]

Enquanto a oferta formativa e o próprio mercado de trabalho se desenvolve, as organizações governamentais têm apostado no recrutamento de *hackers éticos* - os "*hackers* do bem" - para colmatar as falhas dos engenheiros em técnicas de ciberataque. Sendo que qualquer computador é uma potencial ciberarma, e qualquer pessoa com avançado conhecimento de sistemas de informação é um potencial cibersoldado, isso representa um aumento muito grande de possíveis ameaças à segurança nacional, o que exige aos estados apresentar novas medidas de prevenção e proteção dos seus territórios virtuais. Enquanto na guerra tradicional muitas vezes o estímulo militar tem como origem valores como a honra, obediência, camaradagem e lealdade, no caso da guerra virtual as motivações poderão variar de individuo para indivíduo principalmente se, mesmo que o mesmo esteja a desempenhar uma missão em nome do estado, por não ter um percurso militar, poderá não se identificar com aqueles valores.

O conceito de *hacker* [32] enquanto cibernauta especialista em explorar vulnerabilidades informáticas sempre teve uma conotação negativa e criminosa associada, embora os elementos da primeira geração fossem reconhecidos como

[31] Atualmente, em Portugal, o número de oferta de ciclos de estudo relacionados com estas temáticas aumentam ano após ano. Exemplos de universidades que já contemplam estas matérias: Universidade Lusófona, Instituto Politécnico do Cávado e Ave e o Instituto Superior Técnico.

[32] O termo *hacker* é proveniente do jargão inglês de informática e significa "lenhador" (SANTOS, BESSA, & PIMENTEL, 2008). Hack significa cortar de uma forma bruta, o que, conjeturando sobre uma possível interpretação, poderá significar atingir um fim (a penetração de sistemas) de uma forma pouco elegante/correta, neste caso ilegalmente ou antiéticamente.

"*experts*" dentro das suas áreas de investigação tecnológica (SANTOS, BESSA, & PIMENTEL, 2008). É importante esclarecer e distinguir que o hacker, embora possa utilizar as suas competências para fins maliciosos, interessa-se principalmente por testar falhas nos sistemas operativos e superar-se a si mesmo relativamente aos desafios a que se propõe, enquanto que o objetivo do *cracker* é sobretudo violar o sistema com intenções maliciosas, como por exemplo, destruir ou roubar dados.

Ao longo dos anos, tem sido feita uma tentativa de dividir e classificar os diferentes grupos de *hackers* - com base nas suas principais características, motivações e ações – o que permite distanciar os diferentes perfis consoante as suas capacidades mas também valores morais e éticos. Embora frequentemente se associe o *hacking* a uma atividade solitária, seja porque atuam por conta própria e/ou trabalham para organizações, existe também uma comunidade colaborativa por detrás desta atividade. Ainda que não estejam definidos oficialmente nomenclaturas para descrever os tipos de *hackers*, a própria comunidade e autores interessados no tema, foram sugerindo ao longo dos tempos nomes que caracterizam os diferentes grupos.

A uma camada mais superficial, encontram-se os *script kids*. Segundo o *Urban Dictionary*[33], os *script kids* são normalmente adolescentes com pouco conhecimento tecnológico, mas que imitam ou executam códigos de programação de outros, para invadir sistemas computacionais e por isso poderão provocar grandes danos. São normalmente motivados pela fama e gabam-se dos seus feitos. Embora normalmente não pretendam provocar danos de uma forma intencional, a sua presença nos sistemas de informação é igualmente indesejável. A um nível mais profundo, no qual nos iremos focar, encontram-se os "verdadeiros" *hackers*, com sólidos conhecimentos de programação, o que lhes permite desenvolver as suas próprias ferramentas para invasão dos sistemas.

Em oposição ao *cracker*, e numa tentativa de colmatar as falhas de técnicos e engenheiros informáticos nas organizações no que diz respeito a conhecimento e lógica intrusiva, surge a subdivisão de *ethical hacker*. Este é um profissional que utiliza as mesmas técnicas e ferramentas que um *hacker* com intenções maliciosas faria, mas fá-lo de uma forma legítima e autorizada, obedecendo a valores éticos. Estes perfis

[33] *Urban Dictonary* é um dicionário *online* especializado em gírias e expressões em inglês. Fonte: <https://www.urbandictionary.com/define.php?term=script%20kid>.

profissionais são cada vez mais valorizados pelas maiores organizações em todo o mundo porque, tal como na guerra tradicional, conhecer as técnicas e conhecimentos dos inimigos é vital para o sucesso (PALMER, 2001). Embora a oferta formação nesta área esteja a crescer exponencialmente tanto internacionalmente como nacionalmente, existe uma clara falha de recursos humanos para dar resposta às necessidades das organizações, o que implica o recrutamento pouco convencional destes especialistas. Enquanto que as empresas privadas, quando procuram um especialista, fazem-no de forma pública e aberta, desafiando qualquer pessoa a encontrar falhas nos seus sistemas em troca de dinheiro[34], as organizações governamentais têm preferência a contratar a longo termo, considerando que irão lidar com informação sensível com um elevado grau de confidencialidade, e o processo de recrutamento é totalmente confidencial. Os *hackers* éticos têm um papel muito importante na auditoria da segurança da informação, visto que têm uma abordagem dual: detalhada e holística.

A um nível mais profundo, encontramos os *white hat* e *blue hat* como perfis dos *hackers* éticos. O primeiro relaciona-se com aquele que estuda os sistemas, focando-se nas falhas de segurança, e tem como principal tarefa comunicar essas lacunas aos responsáveis da empresa. O segundo perfil orienta-se pelos mesmos objetivos mas o estudo das vulnerabilidades é feito antes do lançamento do sistema para o mercado. Em oposição, os *black hat* são *crakers* que invadem os sistemas, criam vírus com intenções ilícitas como o roubo de dados confidenciais, embora possam existir outros perfis especializados em descodificar informação encriptada ou *softwares* na sua generalidade (LEVY S. , 1984). O *grey hat*, como o nome indica, é um *hacker* intermediário em que embora não seja totalmente ético, porque invade computadores e redes por diversão própria, evita afetar o sistema e não tem como objetivo o armazenamento e a partilha dos dados confidenciais. Nesta categoria, incluo os *phreakers*, especializados em redes telefónicas; os *hacktivistas*, movidos por crenças ideológicas ou religiosas; e os *hackers* de elite, considerados os mais experientes; bem como os *nation states*, que têm como principal alvo setores de infraestruras críticas,

[34] Também chamados de *Bug Bounty Programs.*

militares, serviços públicos ou financeiros.[35] Fi-lo porque a medida ética das ações poderá variar consoante o objetivo, curiosidade e ideologia, ou seja, o mesmo perfil poderá pertencer ao grupo de *hacking* ético ou antiético, consoante o individuo e a própria situação.

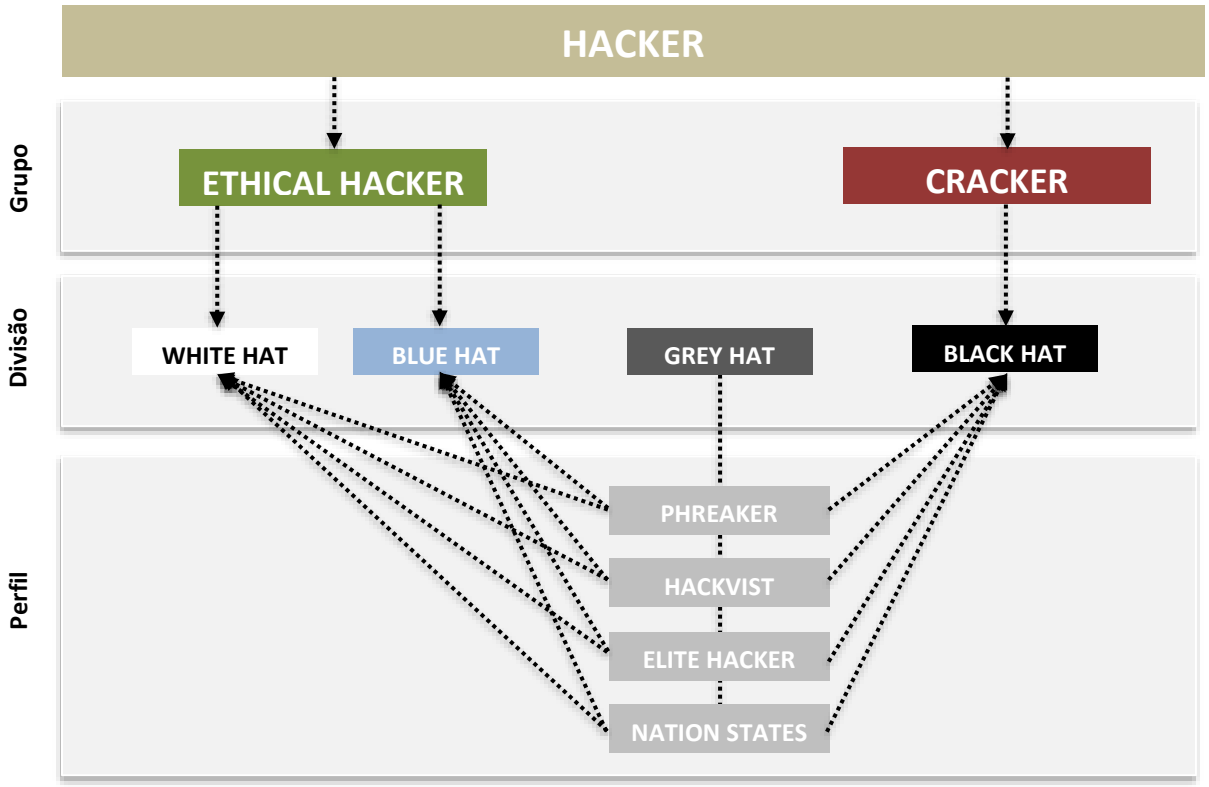

Figura 2 - Sugestão de estrutura de caracterização de *hackers*

Ao longo da pesquisa foram identificada a existência de plataformas[36] *online* para que interessados na matéria desenvolvam e pratiquem as suas técnicas de *hacking*, de uma forma legal. Estas ferramentas assumem uma postura positiva em relação à quebra de barreiras, incentivando a partilha de *websites* com fim a resolver falhas de vulnerabilidade, sempre na perspetiva *learn by doing*.

[35] Os 7 níveis de Hackers. Fonte: <http://www.govinfosecurity.com/blogs.php?postID=1206&rf=2012-02-27-eg>.

[36] Alguns exemplos: Hackerone, Pentest-Tools, Hack the Box e Kali.

III. A CIBERÉTICA COMO GOVERNANÇA DA INFORMAÇÃO

Em consequência do reconhecimento das vantagens da gestão de informação com recurso a um computador, as organizações governamentais, acompanhando a tendência das empresas privadas, passaram a apostar em criar, recolher e manter digitalmente dados de vários níveis de importância. No ciberespaço, a proteção contra o roubo dessa informação é visivelmente mais robusta, pelo menos quando comparada com os mecanismos de existentes. Esses mecanismos de segurança dos documentos físicos - como por exemplo estarem num lugar apenas acessível a determinados elementos dessas organizações e sob uma especial autorização e ocasião – esses eram claramente mais vulneráveis ao roubo quando comparada à possibilidade dessa informação estar protegida por um *software* que apenas permitiria o acesso caso fosse um utilizador autorizado, dono de um *login* pessoal e intransmissível, e com um sistema de autenticação, sem necessidade de intermediários. Essa realidade até pode ter sido realmente vantajosa durante os primeiros anos da utilização dos sistemas computacionais mas, hoje em dia, tendo em conta os desenvolvimentos tecnológicos, a eficácia de proteção é bem mais reduzida. A espionagem e o roubo de identidade são apenas alguns dos exemplos possíveis resultantes do "simples" roubo de uma *password*. Embora eticamente incorretas para alguns, estas infrações e violações de privacidade nem sempre foram contempladas legislativamente e, mesmo nos dias de hoje, não são equiparadas e referidas universalmente como um crime com igual importância àqueles que tomam lugar no mundo físico.

A transformação do crime na nova era informacional foi um tema que foi continuamente estudado e discutido ao longo das duas últimas décadas, com especial incidência nos últimos anos, proporcionalmente ao aumento do número de ciberviolações e, complementarmente, ao acréscimo dos incidentes reportados e expostos pelos *media*. O estudo sobre o cibercrime diferencia-se maioritariamente em duas grandes áreas: (1) a *investigação tecnológica*, mais prática, que incidia na forma como os *hackers* conseguiam invadir os sistemas altamente protegidos; e (2) a *investigação intelectual*, mais abstrata e transversal a temas como o direito e a sociologia, sendo este o tipo de investigação adotado para esta dissertação. Para além

da desconformidade semântica da nomenclatura do conceito, também não existe propriamente um consenso se a ciberguerra é uma ramificação do cibercrime, em que a troca de ataques é focada em estruturas governamentais, mas existe um entendimento global em associar o cibercrime a motivações pessoais e a ciberguerra a discórdias políticas e nacionais. Relacionada direta ou indiretamente com o cibercrime, a ciberguerra foi sendo estudada mais lentamente e hipoteticamente, fruto da falta de provas que levassem a concluir que uma guerra cibernética se avizinha[37]. Não obstante, as primeiras investigações foram essenciais para sensibilizar e estimular a curiosidade de especialistas e académicos e, mais recentemente, em todos aqueles interessados no tema.

A falta de uma declaração oficial de ciberguerra também permitiu uma investigação mais especulativa e holística a outras áreas consideradas subjetivas e dependentes do ponto vista cultural/geográfico adotado pelo investigador, como a ética e os direitos humanos. A subjetividade a que me refiro não é relativamente à definição dos conceitos em si, já que ambos estão universalmente definidos[38], mas à praticidade e aplicabilidade dos mesmos, já que muitos afirmam que a ética depende de valores pessoais (RICH, 2013) e os direitos humanos não são evidentemente exercidos uniformemente pelo mundo, tendo até sido criada uma organização internacional de defesa dos Direitos Humanos – a Amnistia Internacional.

A ética é uma disciplina que tem vindo a ser explorada por alguns autores como parte integrante da ciberguerra, no entanto, a preocupação relativamente à proteção dos direitos humanos é algo que, por enquanto, foi colocado em segundo plano e, por isso, um tema menos explorado academicamente no âmbito da ciberguerra, ainda que cada vez mais haja consciência daquilo que define os dados pessoais e privados e do

[37] Foram documentados ciberataques em que se suspeita que autoria dos ataques seja exterior ao país atacado e com origem em alguma organização ligada ao governo do estado atacante, mas como nunca houve confirmação absoluta da identidade do atacante nem houve um contra-ataque do país lesado, não é unânime considerar que a ciberguerra já começou.

[38] Define-se *Ética* como a disciplina da Filosofia dedicada à abordagem sistemática de identificação, entendimento, análise de um conjunto de valores, como a distinção entre o certo e o errado, e que guia os princípios das ações humanas (RICH, 2013).

Os *Direitos Humanos* são o conjunto dos direitos básicos, civis e políticos, a que todos os seres humanos devem ter acesso, como o direito à vida, à liberdade e à dignidade (Declaração Universal dos Direitos Humanos das Nações Unidas). Fonte: <http://www.un.org/en/universal-declaration-human-rights/>

direito que os seus proprietários devem ter sobre eles. Entre as principais características da conduta ética identifica-se o altruísmo, a consciência e a responsabilidade pelos atos.

Para o contexto militar, Silva (2015) define ética como a reflexão sobre a moral e esta disciplina, em conjunto com os códigos deontológicos, é fundamental para o sucesso das operações militares. Embora não dependentes, a ética e os direitos humanos estão diretamente interligados entre si, pois a falta de ética das organizações governamentais (p.e. em situações de ciberataque ou ciberdefesa) poderá comprometer os direitos humanos – nomeadamente a privacidade dos indivíduos - a fim de um *bem maior*.

Autores com formação em Sociologia, Psicologia, Direito e, maioritariamente, Filosofia e Tecnologias de Informação, mostram-se os principais responsáveis pelo debate do tema e pertencem a diferentes tipos de organizações (governamentais, políticas ou militares). Joseph Migga Kizza, Andrew Colarik, Lech Janczewski são apenas alguns dos autores que, embora especializados em tecnologia, como informática, contribuíram para a discussão relativamente aos problemas éticos e sociais na sociedade de informação, sobretudo em contexto de ciberguerra. No que toca aos militares, pude observar que muitos dos autores que abordam estes assuntos, possuem uma direta ligação com as próprias organizações, o que significa que as próprias Forças Armadas incentivam à pesquisa e divulgação do debate.

Em 2003, um dos objetivos da comunidade internacional, incluindo especialistas em informação e filosofia, seria chegar a um consenso relativamente ao *core* dos valores e princípios éticos na sociedade de informação (Floridi, 2002) e, até hoje, apesar das iniciativas de cooperação internacional e definição de princípios base de atuação, atingir o consenso pleno é muito difícil. Floridi, filósofo italiano e pioneiro no campo da Filosofia e Ética de Informação, menciona em 1999 a necessidade de conferir princípios como o respeito, conservação e valorização à própria informação – princípios esses que podem ter sido postos em causa com a alteração do valor económico da informação e com o surgimento dos *big data*. Para além deste autor, não podia deixar de realçar uma das principais referências para este tema, Randall Dipert, especializado em ética militar, e ex-Professor na U.S. Military Academy em West Point, de 1995 a 2000[39]. Maria Rosaria

[39] Fonte: <https://dipert.org/>.

Taddeo, autora do livro "*The Ethics of Cyber Conflicts: An Introduction*", publicado em 2017, e filósofa de formação, tem também produzido ao longo dos últimos anos artigos sobre as práticas de cibersegurança e ciber-conflitos, conferindo-lhes uma análise ética.

De acordo com Reynolds (2011), a Moralidade diz respeito às convenções sociais sobre aquilo que é certo ou errado e, por serem tão amplamente partilhadas, são a base daquilo que chamamos senso comum. A Ética são crenças relativas ao comportamento das normas sociais, subjetivas à interpretação individual, sendo esta baseada em influências familiares, crenças religiosas, valores pessoais ou experiências de vida. O sistema de valores de uma pessoa varia consoante as suas *virtudes* – hábitos que levam-na a fazer aquilo que é "aceitável" - e *defeitos* – hábitos que levam-na a fazer aquilo que é "inaceitável" - mas também consoante a sua *integridade* – capacidade de atuar de igual forma em todas as situações. A um nível menos enigmático, a Carta dos Direitos Fundamentais da União Europeia[40], proclamada em 2000, representa o grande esforço em proteger internacionalmente os direitos humanos, através do estabelecimento determinados valores e princípios comuns para a comunidade que devem ser implementados. Ainda que os direitos não sejam legalizados e aplicados em todos os países, os Direitos Humanos conferem uniformidade de princípios com um nível de obrigatoriedade internacional (ainda que não punível por lei em todos os países). O respeito pela dignidade, liberdade, igualdade, solidariedade (em que se inclui o direito à informação), cidadania e justiça são apenas alguns dos diretos fundamentais realçados na Carta.

As Forças Armadas, como uma das partes mais interessadas em compreender este fenómeno, têm vindo a debater e a contemplar o tema da ciberguerra em conferências, palestras e formações académicas. Num plano mais particular, a influência direta ou indireta nos civis, é um tema que tem sido investigado, não só por militares como outros especialistas. De acordo com Neil Rowe (2010), a ciberguerra não tem como principal alvo o pessoal militar, mas sim o seu *software* e os seus dados. Contudo, considerando que as organizações militares (e governamentais) usam principalmente o mesmo *software* que os civis, e os computadores comuns são muito mais vulneráveis ao ataque, os civis e os seus computadores poderão ser o veículo para um ataque com

[40] Fonte: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>.

outras proporções. À parte da forma como os civis poderão contribuir para uma ciberguerra, seja para moldá-la ou para instigá-la, também existe uma real preocupação relativamente aos civis enquanto dano colateral. Para tal, Bertoli & Marvel (2017), ambos formados em engenharia elétrica mas com um percurso ligado a organizações governamentais e militares, definiram um modelo que avalia e compara os efeitos da ciberguerra *versus* a guerra tradicional e que permite prever o risco, contemplando o contexto em que o episódio se passa.

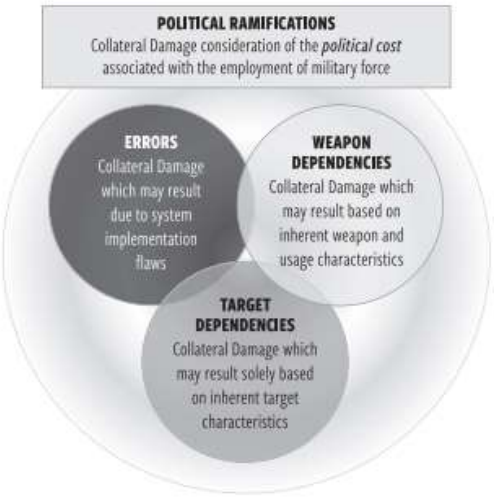

Figura 3 - Taxonomia geral do Dano Colateral por Bertoli & Marvel (2017)

O facto de não dominar outros idiomas limitou a minha pesquisa literária à língua portuguesa, espanhola e inglesa. Por essa razão, as conclusões que irei apresentar neste parágrafo acerca das nacionalidades dos autores e investigadores desta matéria poderão ser limitadas. Efetivamente, e inevitavelmente por ser a "língua universal", grande parte dos estudos estão em inglês – o que acaba por facilitar a troca de conhecimento entre investigadores. Aparentemente, a maior parte dos autores que escrevem sobre estes assuntos são americanos ou britânicos, contudo, não poderei comprovar isso tendo em conta a extensão da informação recolhida. Em especial, os Estados Unidos parecem estar incluídos e referenciados na maior parte das reflexões e isso pode ser por duas razões essencialmente: porque os próprios EUA são os maiores interessados que se investigue sobre o tema; e/ou porque são um país com uma história "pública" mais rica, quando comparados a outros com um regime ditatorial como a Coreia do Norte, por exemplo. Em Português, estuda-se o tema da ciberguerra sobre a

perspetiva das Relações Internacionais e da História. Em 2013, Ramos estudou como a vigilância em massa atua a favor de determinados agentes na obtenção de informações que possibilitem uma posição de vantagem na ciberguerra. Contudo, Ramos foca-se no estudo de caso do ciberataque do Stuxnet ao Complexo Nuclear de Natanz no Irão, em 2010, o que acaba por não ser diretamente relacionado com o tema desta dissertação, mas que acabou por contribuir com diferentes argumentos e fundamentos literários. Através de Ramos (2013) descobri a existência de um sistema de avaliação e medição de forças na ciberguerra, denominado *Overall Cyber War Strength*. De forma a obter um resultado o mais realista possível, e para além do poder de ofensa, os autores Clarke[41] & Knake (2014), tiveram em consideração outros fatores como a *defesa* - medida que verifica o nível de capacidade de uma nação em responder ao ataque com vista à mitigação e bloqueio do mesmo – e *dependência* – medida que afere o quanto uma nação está conectada e dependente de redes e sistemas vulneráveis em caso de ciberataque. Os autores americanos estudaram cinco regiões: Estados Unidos, Rússia, China, Irão e Coreia do Norte, sendo que a Coreia do Norte tem uma avaliação geral mais positiva (18 pontos), seguida pela China (15 pontos). Para efeitos desta dissertação, apresento em seguida os resultados obtidos para os Estados Unidos e Rússia.

PAÍS	EUA	RÚSSIA
CIBEROFENSA	8	7
CIBERDEPENDÊNCIA	2	5
CIBERDEFESA	1	4
TOTAL	**11**	**16**

Tabela 3 - Comparação de forças entre os EUA e a Rússia segundo Clarke & Knake (2014)

Observando a urgência em regulamentar a ciberguerra, um grupo de especialistas independente em lei internacional junta-se em 2009, a convite da *North Atlantic Treaty Organization - Cooperative Cyber Defence Centre of Excellence* (NATO

[41] Assesor do ex-presidente dos EUA George W. Bush em matérias de ciberterrorismo, durante o 9/11.

CCD COE), com o objetivo de debater de que forma a lei era aplicável na resolução de ciberconflitos e os limites do uso da força[42]. Do decorrer de diversas reuniões, em 2013 foi concluído o *Manual on the International Law Applicable to Cyber Warfare* que avalia a aplicabilidade do direito internacional no ciberespaço, tendo sido publicada uma segunda versão que apresenta uma análise legal, técnica, estratégica e operacional de cenários cibernéticos. O *Manual de Tallin*[43], como também é conhecido, não se trata de um tratado ou um documento legal vinculativo mas antes uma instrução na conduta de ciberoperações[44] e clarificação da lei neste âmbito. Este documento visa examinar as razões justificáveis para se entrar em guerra (*jus ad bellum*) e o Direito Humanitário Internacional (DIH), que define os princípios que devem ser tidos em conta em conflitos armados (*jus in bello*), regulando assim a maneira como a guerra é conduzida. O DIH destina-se a proteger as vítimas do conflito armado (SCHMITT, 2013), independentemente da sua posição filiação partidária. Assim sendo, as doutrinas *jus ad bellum* e o *jus in bello* devem manter-se independentes.[45]

O Manual de Tallin é uma fonte de referência para esta investigação e foi feito um esforço para verificar a conformidade das ciberestratégias dos Estados Unidos, Rússia e Portugal com este guia, todavia, é importante referir que dentro do âmbito desta dissertação não foi possível produzir uma verificação e análise exaustiva entre a vertente prática e a teórica. Em seguida são apresentadas algumas ideias-chave do Manual de Tallin relacionadas com a ciberguerra e as implicações nos direitos humanos:[46]

---

[42] Citando Passos (2016), Schmitt apresenta seis requisitos para diferenciar o uso da força do ataque armado: gravidade, iminência, caráter direito, caráter invasor ou intrusivo, mensuralidade ou extensão e presumível legitimidade.

[43] Tallin (capital da Estónia) foi o local onde este manual foi assinado, explicando esta nomeação complementar.

[44] De acordo com o Manual de Tallin, ciberoperações são o emprego de capacidades cibernéticas com o objetivo principal de alcançar objetivos no ciberespaço ou pelo uso do ciberespaço.

[45] De acordo com o Comité Internacional da Cruz Vermelha. Fonte: <https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0>.

[46] Os títulos laterais dizem respeito ao capítulo correspondente no Manual, contudo, as regras poderão ter sofrido alterações para adaptações à lingua portuguesa e de forma a concentrar ideias. Não foram mencionadas todas as regras, apenas aquelas que estavam diretamente relacionadas com o propósito desta investigação.

MANUAL DE TALLIN	
ESTADOS E O CIBERESPAÇO	Sem prejuízo das obrigações internacionais aplicáveis, um Estado pode exercer sua jurisdição: (a) Sobre pessoas envolvidas em atividades cibernéticas no seu território (físico); (b) Sobre a infraestrutura cibernética localizadas no seu território (físico); (c) Extraterritorialmente, de acordo com o direito internacional.
	O mero fato de que uma ciberoperação tenha sido lançada ou [...] originada na infraestrutura cibernética do governo não é evidência suficiente para atribuir a operação a esse Estado mas é uma indicação de que o Estado em questão está associado à operação. Todavia, se a ciberoperação foi encaminhada através da infraestrutura cibernética localizada num Estado não é prova suficiente para atribuir a operação a esse Estado.
	Um Estado afetado por um ato internacionalmente ilícito pode recorrer a contramedidas proporcionais, incluindo contramedidas cibernéticas, contra o Estado responsável.
O USO DA FORÇA	Uma ciberoperação constitui um uso de força quando a sua escala e os seus efeitos são comparáveis a operações não-cibernéticas que se elevam ao nível do uso da força.
	Um Estado que é alvo de uma ciberoperação que se eleva ao nível de um ataque armado pode exercer seu direito inerente de autodefesa.
	No exercício do seu direito de autodefesa, o uso da força em operações virtuais realizadas por um Estado deve ser necessário e proporcional.
A LEI DO CIBERCONFLITO ARMADO	As ciberoperações executadas no contexto de um conflito armado estão sujeitas à lei do conflito armado.
	Comandantes e outros superiores são criminalmente responsáveis por ordenar ciberoperações que constituam crimes de guerra. São igualmente responsáveis se tiveram conhecimento de que os seus subordinados planeiam cometer, estão a cometer ou cometeram crimes de guerra e não aplicaram medidas de prevenção ou castigaram os responsáveis.

Tabela 4 - Diretrizes do Manual de Tallin, parte I

MANUAL DE TALLIN	
CONDUTA DE HOSTILIDADES	Os civis (maiores de 15 anos) não estão proibidos de participar diretamente de ciberoperações que resultem em hostilidades, mas perdem a sua proteção contra ataques durante o tempo em que participarem, tornando-se combatentes.
	A população civil não deve ser objeto de ciberataque nem os seus pertences. Considera-se como pertences civis (incluindo computadores e redes de computadores) aqueles que por natureza, localização, propósito ou uso, não contribuem efetivamente para a ação militar e cuja destruição total ou parcial, captura ou neutralização, nas circunstâncias dominantes na época, não oferece uma vantagem militar competitiva.
	Em caso de dúvida sobre se um objeto normalmente dedicado a propósitos civis está a ser usado para fazer uma contribuição efetiva para a ação militar, a determinação deve ser feita após uma avaliação cuidadosa e, em dúvida, deve assumir-se que não está.
	Relativamente aos meios (armas) e métodos (táticas) de guerra, é proibido privar deliberadamente os civis de nutrição (incluindo água) como método de ciberguerra.
	Um ciberataque que trata como alvo único objetos militares claramente discretos na infraestrutura usada principalmente para fins civis é proibido se isso prejudicar os civis ou os seus objetos.
	Aqueles que planeiam, aprovam ou executam um ciberataque devem cancelar ou suspender o ataque se for evidente que: (a) o objetivo não é militar ou o assunto está sujeito a proteção especial; ou (b) o ataque pode causar, direta ou indiretamente, perda acidental de vida civil, ferimentos a civis, danos a objetos civis ou uma combinação dos mesmos que seriam excessivos em relação à vantagem militar concreta e direta prevista.
	A ciberespionagem e outras formas de recolha de informações direcionadas a um adversário durante um conflito armado não violam a lei do conflito armado.
	Um membro das forças armadas envolvido em ciberespionagem em território controlado pelo inimigo perde o direito de ser um prisioneiro de guerra e pode ser tratado como espião se capturado antes de voltar a juntar-se às forças armadas para as quais ele pertence.

Tabela 5 - Diretrizes do Manual de Tallin, parte II

MANUAL DE TALLIN	
DETERMINADAS PESSOAS, OBJETOS E ATIVIDADES	As partes de um conflito armado devem respeitar e proteger bens culturais que possam ser afetados por ciberoperações ou que estejam localizados no ciberespaço. Particularmente, é proibido de usar propriedade cultural digital para fins militares
	O ambiente é um objeto civil e, como tal, goza de proteção geral contra ciberataques e os seus efeitos. Qualquer meio ou método de guerra que intencionalmente, ou expetavelmente, cause danos a longo prazo ao ambiente são proibidos
	A punição coletiva, por exemplo penalização de civis por atividades em que não estiveram envolvidos, é proibida

Tabela 6 - Diretrizes do Manual de Tallin, parte III

É notória a preocupação de alguns governos relativamente à descentralização do poder numa rede anárquica e, ao longo das últimas décadas, têm vindo a ser feitos esforços para controlo dos limites tecnológicos. As sugestões de regulamentação, legislativa e/ou ética, têm provocado momentos de tensão, controvérsia e desacordo justificado pelas necessidades de segurança nacional, não existindo consenso. Spinello (2010), invoca a *framework* de Larry Lessig, em "*Code and Other Laws of Cyberspace*" (1999), que estabelece a *lei* e *normas* como sendo duas forças[47] modeladoras do comportamento dos indivíduos. Enquanto as leis são imposições ou ordens impostas à sociedade e controladas por uma entidade de alta autoridade (como o governo), as normas sociais são expressões informais pré-definidas da comunidade, que se traduz, numa maneira mais simples, no conjunto de regras ou princípios que definem os limites daquilo que é aceitável quando vivemos em sociedade. Este sentido de normalidade é refletido nos comportamentos da maioria dos indivíduos de uma sociedade, contudo, qualquer desvio na manifestação ou violação da norma social acarretará uma condenação social mas nunca uma legal. Admitindo a impossibilidade de regulamentação legislativa, é previsível que o compromisso social não seja suficiente para impedir atos bélicos. A supramissão de um país é proteger os seus territórios e os

[47] O autor também refere outras duas forças: o mercado e o código (referente à arquitetura de computadores) mas por não apresentarem relevância para o contexto da investigação não foram consideradas.

seus cidadãos e, por essa razão, nenhum país confia a sua segurança a outros, sejam eles inimigos ou não, com base nas normas socialmente aceites e definidas, porque estas poderão variar culturalmente e, mesmo sendo iguais, nada garante que elas sejam cumpridas. Para além disso, a ética tende a cobrir situações comuns, frequentes e partilhadas por muitos mas, por vezes, estes princípios não são aplicáveis a novos cenários, especialmente quando existe um conflito de *meio* vs. *fim* (cibervigilância vs. defender de um novo perigo).

IV. A CIBERGUERRA COMO O NOVO DESAFIO À SEGURANÇA NACIONAL

Ainda que conceptualmente se fale em guerra de informação desde o fim do século XIX, tem sido notoriamente crescente a preocupação relativa não só às consequências, mas também à frequência de ataques a sistemas de informação. A informação *aportou* e *aporta* valor estratégico para um país, independentemente do mesmo adotar uma postura ofensiva ou defensiva. Segundo Gian Piero Siroli, entende-se a guerra da informação como o "conjunto de atividades que visam negar, corromper ou destruir as fontes de informação do adversário", tanto das operações de defesa como de ataque (HALPIN, TREVORROW, WEBB, & WRIGHT, 2006). A ciberguerra surgiu como uma evolução natural deste fenómeno, mas agora sem a imposição de "limites territoriais, com objetivos fluidos de largo espectro estratégico [.] e, para além dos comandos clássicos, por comandos descentralizados distribuídos por células militares que se socorrem de TI para atuar" (SANTOS, BESSA, & PIMENTEL, 2008). Ainda que não tenha sido possível encontrar um estudo que confirme a espionagem como sendo o crime digital estatisticamente mais frequente, a verdade é que, tanto na guerra convencional como na nova guerra, reconhecer o inimigo e o conhecimento que detêm é vital para o sucesso e por essa razão calcula-se que seja o ataque/objetivo mais habitual e repetido. Esta ideia foi também confirmada por Santos, Bessa e Pimentel (2008), tendo eles referido que "quanto mais hábil um exército for na aquisição e gestão da informação [...] maior será a sua capacidade de minimizar as suas fraquezas [...] e maior a sua capacidade de identificar as vulnerabilidades do inimigo e potenciar o seu aparelho e força militar contra ele".

Ainda que a ciberguerra possa ser definida genericamente como qualquer conflito virtual com motivações políticas e/ou militares e iniciado com um ataque aos sistemas de informação digitais de um inimigo, fazendo um "uso disruptivo de ferramentas de manipulação em redes de computadores" (RUHMANN, 2013), esta explicação não é definitiva. Isto deve-se principalmente ao carácter volátil da *internet* e daquilo que está relacionado com a mesma, incluindo a maneira como a sociedade lida com a informação, tornando a discussão hipotética, inconclusiva e facilmente obsoleta.

É relativamente fácil distinguir cibercrime de ciberterrorismo pela sua

motivação, pessoal ou política respetivamente, contudo, considerando que a ciberguerra envolve igualmente a esfera política dos países, torna-se mais difícil à partida diferenciar os dois fenómenos. Tal como o ciberterrorismo, o foco da ciberguerra é lesar o país inimigo, todavia, o modelo de operação é diferente, sendo que é esperado um nível de violência direto e físico bastante diferente. No ciberterrorismo, um indivíduo ou grupo de indivíduos atacam o inimigo em representação do seu país/crença. Neste caso, o inimigo é preferencialmente alvo(s) não-combatente(s) (SANTOS, BESSA, & PIMENTEL, 2008), ao contrário da ciberguerra que, na teoria, deveria limitar-se a confrontos entre exércitos virtuais, sendo a manipulação de fontes de informação o foco principal e não a morte ou destruição de propriedade de civis (que pode acontecer mas é considerado dano colateral).[48]

A *nova* guerra é diferenciada por uma multiplicidade de tipos de unidades de combate resultantes de colaborações públicas e privadas (KALDOR, 2007) e que visam tanto a defesa como o ataque face a um determinado alvo, seja a oposição um individual ou um grupo de indivíduos. O relacionamento com entidades não militares permite um maior conhecimento situacional da segurança nacional ou internacional, maximizando o potencial bélico da nação e tornando os diferentes meios militares interoperáveis (SANTOS, BESSA, & PIMENTEL, 2008). Adicionalmente, os autores identificam essa "parceria" como uma necessidade para a tomada de decisões militares, baseadas no processamento de dados rápido e eficaz, "em tempo real de acordo com processos de gestão de conhecimento apoiados em sistemas de apoio à decisão que conduz[e]m à obtenção de maiores vantagens militares sobre o adversário". Todavia, no caso particular da ciberguerra, não é tão nítida a real entidade do inimigo nem o seu propósito. Tendo em conta essa nova realidade, podemos observar que, a introdução do ciberespaço enquanto novo domínio de guerra, veio alterar a postura do inimigo e, consequentemente, a própria dinâmica de confronto. Enquanto que na guerra tradicional os próprios países admitiam serem inimigos uns dos outros, e de certa forma celebravam-no como se fosse um ato de dignidade e honra, na ciberguerra é precisamente o contrário – o objetivo é ninguém assumir a culpa, deixando que as especulações alimentem o medo. A *velha* guerra também pressupunha,

[48] Fonte: <https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#>.

ocasionalmente, uma frente assumida e composta por países aliados, o que agora não é hábito, embora continuam a existir cooperações internacionais como no fundo opera a União Europeia e a NATO.

A teorização sobre a evolução e modernização da guerra, com recurso à alta tecnologia, é uma necessidade do tempo presente mas esta reflexão e previsão tem vindo a ser feita durante as últimas trinta décadas. Ainda que teorização pelo tema tenha sido relevante para as organizações militares, é perfeitamente normal que agora possam ser consideradas obsoletas, não apenas porque a tecnologia evoluiu de uma forma que poderia não corresponder às previsões, mas também porque determinados eventos na história mundial moldam e definem novos paradigmas militares, originando novas ramificações de realidades paralelas. Os eventos a que me refiro poderão ser situacionais e diretos, como o ataque terrorista 9/11, como menos concretos e mais duradouros, como a proliferação dos jogos de guerra nas últimas duas décadas. Jari Rantapelkonen, em "*Cyberwar, Netwar and the Revolution in Military Affairs"* (2006, p.5) argumenta que "a guerra contra o terrorismo não é um problema de território mas sim uma criação dos *media* na qual a tecnologia do mundo virtual é concedida com uma dimensão virtuosa ou ética". Em exemplo acrescenta que, em 2001, a empresa de relações públicas Rendon Group foi contratada pelo Pentágono [49] para criar uma imagem positiva de novas formas de guerra.

Contrariamente à guerra tradicional, a ciberguerra tem dimensões mais dificilmente mensuráveis, contudo, poderá causar igualmente danos irreversíveis às estruturas vitais da sociedade. A existência de uma rede de computadores crítica para o funcionamento do país é extremamente aliciante e vantajosa para os inimigos, tendo em conta que os esforços se focam apenas em atacar um determinado alvo. Por saberem isso, e no sentido inverso, as organizações governamentais, em conjunto com os recursos militares, têm vindo a apostar cada mais na ciberdefesa dos seus territórios virtuais, com recurso a infraestruturas de tecnologias poderosíssimas que pretendem responder a incidentes virtuais de uma forma mais rápida e eficaz. *Counter-cyber* poderá ser facilmente um termo utilizado e interpretado como sinónimo de ciberdefesa, mas existe uma conotação ligeiramente diferente. *Counter-cyber* implica um ato de defesa

[49] Pentágono é o nome dado à sede do Departamento de Defesa dos Estados Unidos.

em função de um ataque inimigo, ou seja, é um contra-ataque e tem uma postura ofensiva associada[50]. Uma ciberguerra poderá ser uma extensão ou extensível à guerra tradicional, mas também poderá ser totalmente autónoma, e o confronto ser apenas virtual.

Segundo Santos, Bessa e Pimentel (2008), países como os Estados Unidos, Rússia, China "são praticamente inexpugnáveis [e impenetráveis], em termos militares, ao nível das Tecnologias de Informação" pois as suas infraestruturas de rede não estão conectadas ao ciberespaço. Contudo, isso significa que os adversários passam a orientar os seus esforços contra alvos não militares, como os sistemas terminais (computadores, servidores e *smartphones*) de organismos públicos, empresas privadas ou até mesmo civis, como *meio para atingir um fim*, sendo a assimetria de alvo o principal desafio à segurança nacional: todos podem ser atacados, a qualquer momento e a partir de qualquer lugar. Para além dos desenvolvimentos tecnológicos, a acessibilidade e conetividade passaram a exigir um constante estado de alerta e monitorização do ambiente digital, podendo incluir o supervisionamento de utilizadores finais (civis) pelo seu caracter frágil, devido a estarem pouco sensibilizados para as necessidades de segurança, fazendo deles uma "presa" fácil para atacantes.

Um só clique pode ser suficiente para afetar as estruturas críticas de um país, como, por exemplo, os sistemas de transporte e distribuição de eletricidade que têm como principal objetivo suportar outros sistemas *core*, transversais a todos os civis, que garantem o bem-estar da sociedade, seja ele económico ou social. A perturbação ou destruição de uma estrutura crítica tem um impacto muito significativo no país (quer o serviço seja fornecido por uma estrutura publica ou privada) e, por essa razão, são os alvos favoritos quando o objetivo é atingir o país no seu conjunto. Supondo que muitos sistemas comunicam em rede, através da internet, o ataque pode tomar proporções ainda maiores: maior rapidez de ataque, eficiência e mais ataques em simultâneos. De forma a reforçar a soberania do país, no passado mês de Fevereiro, o Presidente Vlamidir Putin admite um plano de contingência que consiste na desconexão da Rússia do resto do mundo. A hipotética criação de um sistema individual de redes de

[50] De acordo com o Memorando "*Joint Terminology for Cyberspace Operations*" (2010). Fonte: <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

computadores interligados com os seus próprios protocolos irá provocar consequências diretas na esfera política e económica local e global, e indiretas, como o impacto nos serviços secretos dos outros países. Todavia, a Rússia não pretende isolar-se do ciberespaço mas sim tornar-se independente e defender melhor as suas fronteiras virtuais, o que poderá exigir a definição de novas ciberestratégias de ataques dos países adversários.

A ciberguerra apresenta-se como o novo desafio de segurança nacional e já existem evidências que comprovam o impacto nas relações internacionais. Em seguida são identificados quatro ataques dos mais marcantes na ciberguerra:

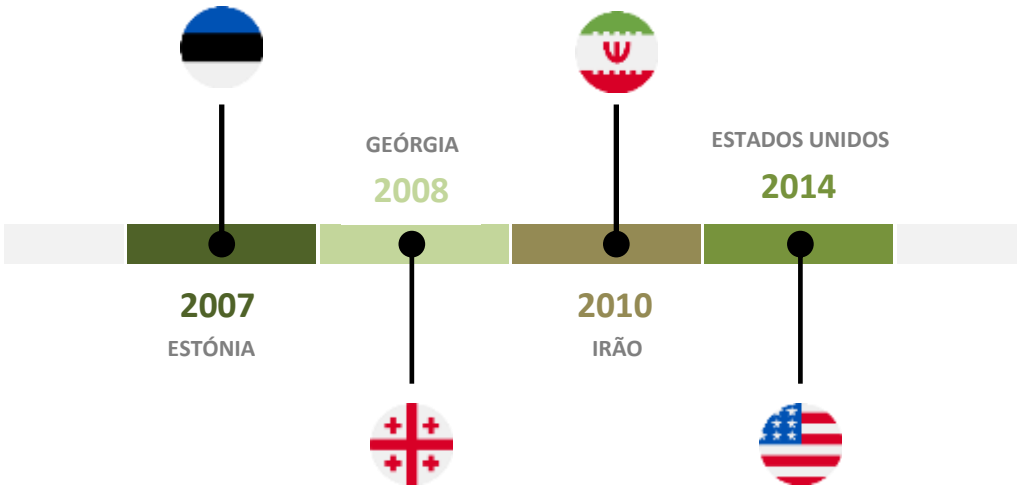

Figura 4 - Cronologia dos principais ciberataques

ESTÓNIA

A Estónia foi o primeiro país a sofrer um ciberataque com proporções nacionais. Os sistemas informáticos estonianos, pertencentes a entidades públicas e privadas, sofreram uma série de ataques simultâneos de negação de serviço (DoS) que perturbaram o funcionamento do país. Estes ciberataques decorreram durante sensivelmente três semanas, ainda que com diferentes intensidades, e os *web servers* eram o principal alvo.

Rain Ottis[51], ao abrigo da NATO CCD COE, analisa este ciberataque mencionando três hipotéticos cenários:[52]

HIPÓTESE	ANÁLISE
O evento foi uma operação de informação Russa contra a Estónia	Este cenário é frequentemente justificado enquanto punição pela realocação da estátua representativa da conquista e ocupação soviética (atual Rússia). A Rússia negou um envolvimento direto ou indireto com estes ciberataques, contudo, não foram observadas medidas de mitigação e cooperação das autoridades russas, o que poderá representar uma postura de apoio aos ataques.
O evento foi uma operação incriminar a Rússia como atacante	A rivalidade entre os dois países é conhecida internacionalmente e, por isso, poderia ser utilizada facilmente como fundamento para culpabilizar o governo Russo, não obstante, não justifica a falta de cooperação nas investigações nem a origem dos ataques em território russo, tornando este cenário implausível.
O evento foi uma resposta espontânea e *grass rooted* à política do governo estoniano	Este cenário justificaria o facto de nenhuma organização ter assumido a responsabilidade relativamente aos ciberataques, porém, como já anteriormente mencionado, na ciberguerra o inimigo é dificilmente identificado. Esta teoria exigiria ações de sujeitos independentes sem afiliação ao governo (*grass rooted*) e, uma vez que foi verificada a falta de apoio da Rússia, esta teoria é fortemente improvável.

Tabela 7 - Análise de cenários do ciberataque à Estónia

Estes ataques de negação de serviço foram o primeiro exemplo de uma ciberoperação a larga escala em que o alvo de ataque era um país mas, independentemente das motivações políticas, o campo de batalha escolhido não foi ao acaso, considerando que a Estónia era um dos países mais digitais da Europa. Tanto naquela altura como agora, a Estónia não é um dos países com maior capacidade financeira mas aquele ciberataque não impediu o contínuo forte investimento em tecnologia.

[51] Professor de Gestão de Cibersegurança na Universidade de Tecnologia de Tallin.

[52] Fonte: <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>.

GEÓRGIA

Sensivelmente um ano após os ataques à Estónia, os territórios georgianos estavam a ser invadidos pelo exército Russo. Foi também durante esta altura que a Geórgia foi alvo do primeiro *Computer Network Attack* (CNA) a larga escala por *hacker*s russos, maioritariamente com ataques de DoS. Não se verificou assumidamente uma conexão direta com o governo russo, contudo, foi evidenciada a relação com a campanha militar. Shakarian (2011) na sua análise em "*The 2008 Russian Cyber Campaign Agaisnt Georgia"*, explica que, contrariamente à Estónia, a Geórgia apresentava redes muito mais frágeis, o que facilitou a desconexão e o isolamento temporário do mundo exterior, sendo esse o objetivo primário. Os ataques dirigiam-se a *websites* governamentais e de media, tendo sido mais tarde alargado a outras entidades, através de uma campanha de *e-mail spam*, que promovia o recrutamento de *hackvistas* que promovessem a difusão dos ataques. O autor ilustra algumas teorias com possíveis evidências, segundo diferentes níveis de atribuição da autoria do ataque:

ATRIBUIÇÃO	ANÁLISE
Hackivistas patrióticos	Foram identificadas duas fases de ataque com diferentes características, o que significa que, embora possa ter havido participação de *hackvistas* pelo recrutamento, não existem evidências de envolvimento na primeira fase da ciberoperação.
Crime organizado russo	A utilização de *botnet*s e o facto de *websites hackvistas* (p. e. StopGeorgia.ru) estarem ligados a organizações criminosas torna esta hipótese mais plausível. Segundo o meu entendimento, o autor sugere que, em vez de uma atribuição única, estes ataques são fruto de uma parceria com diferentes competências e objetivos.
Crime organizado a pedido do governo	Esta teoria foi mencionada por diferentes autores que alegam uma ligação do presidente Vladimir Putin com grupos de crime organizado tais como a Russia Business Network, todavia, não foram encontradas provas que lhes confiram a atribuição do CNA.

Tabela 8 - Análise de cenários do ciberataque à Geórgia

Em suma, estando ou não o governo russo envolvido, os ciberataques fragilizaram a diferentes níveis a Geórgia, beneficiando a operação russa. Shakarian acrescenta que este episódio impacta diretamente a cibervigilância da *network* civil a fim de mitigar novos ataques.

IRÃO

Stuxnet foi o primeiro *worm* projetado especificamente para atacar uma infraestrutura industrial crítica. Este vírus possui um *malware* específico para atingir sistemas configurados que controlam e monitorizaram processos industriais da marca Siemens. Em 2010, o Centro Nuclear do Irão, que utilizava os sistemas da marca alemã, foi uma das organizações infetadas com o Stuxnet e isso provocou distúrbios nas centrifugadoras de enriquecimento de urânio na fábrica de Natanz. Segundo o embaixador russo na NATO, este vírus "poderia levar a um novo Chernobil[53]" e, se não tivesse havido controlo da propagação (que chegou a computadores pessoais) esta poderia ser uma realidade bem provável.[54] A criação deste vírus tão poderoso foi atribuída a Israel e aos Estados Unidos, ao abrigo da parceria *Operation Olympic Games* iniciada pelo antigo presidente George W. Bush.[55]

ESTADOS UNIDOS DA AMÉRICA

Em 2014 ocorre um dos ciberataques mais mediáticos internacionalmente. Ainda que o alvo não seja uma estrutura nacional, como nos exemplos anteriores, por se ter verificado divulgação voluntária de dados confidenciais de civis e existirem motivações políticas por de trás deste ataque, pode também ser utilizado como um exemplo de ataque em cenário de ciberguerra. O cancelamento da estreia e distribuição do filme norte-americano *The Interview*[56] foi o culminar de uma série

[53] Acidente nuclear catastrófico, ocorrido na União Soviética (atual território ucrâniano) em 1986, resultado da explosão do reator da Central Nuclear de Chernobil.

[54] Fontes: <https://www.bbc.com/news/world-middle-east-11414483> e <https://www.bbc.com/news/technology-12465688>.

[55] Fonte: <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.

[56] Sátira política que tem como *plot* o homicío do líder da Coreia do Norte Kim Jong-Un.

ciberataques à produtora Sony Pictures. Para o país liderado por Kim Jong-Un, o lançamento do filme "era uma declaração de guerra e não iria ser ignorada ou tolerada", tendo sido diplomaticamente apresentado o pedido de cancelamento do filme mas o mesmo não foi aceite, embora tenham sido tomadas medidas para minimizar suscetibilidades, como não divulgar o filme em determinadas salas de cinema (SIBONI & SIMAN-TOV, 2014). Pouco depois, os sistemas de informação da Sony Pictures são *hackeados* e é disponibilizada publicamente informação confidencial não só do negócio mas também dos seus colaboradores. [57] Este foi um dos poucos casos em que, para além da pressão sobre uma empresa privada, foi também feita uma ameaça de danos físicos aos civis e um ataque à liberdade de expressão, um direito humano contemplado na realidade norte americana.

A iminência de um possível ataque obriga os estados a munirem-se de capacidades de ciberdefesa. Genericamente, a guerra implica o envolvimento de uma ou mais países e nos exemplos referidos não houve contra-ataque mas foram tomadas medidas preventivas e de proteção em todos eles (ciberdefesa) e, por isso, teoricamente houve resposta ao conflito. Todavia, não existe acordo internacional relativamente se este tipo de ciberoperação possa ser considerado um ato de ciberguerra mas é consensual que importa reconhecer se o incidente é da responsabilidade da aplicação da lei ou dos militares (Mike Reagan, 2012), quais são as metodologias, metas e consequências da ciberoperação (Alex Seger, 2012) e deverá ser sempre feita uma investigação mais profunda antes de rotular o evento (Richard Stiennn, 2012).[58]

[57] Por exemplo: dados pessoais de colaboradores; *e-mails*; salários; argumentos; cópias de filmes ainda não divulgados; entre outros.

[58] Este levantamento de opiniões foi efetuado por Passos (2017, p. 11) em tradução do autor.

V. CIBERVIGILÂNCIA COMO AMEAÇA À PRIVACIDADE

A vontade quase intrínseca do ser humano em se mostrar aos outros não é algo recente que surgiu com as redes sociais e nem é algo que signifique forçosamente afirmação e competição perante os outros, como em tempos. Num mundo partilhado, é importante que, embora existam traços que reflitam o contexto onde nos inserimos, todos nós tenhamos uma identidade única, pessoal e intransmissível e sejamos reconhecidos de imediato por isso. Mas se por um lado queremos que os outros nos identifiquem pela nossa individualidade, *por outro*, completamente contraditoriamente à ideia anterior, observa-se uma crescente preocupação nos últimos anos relativamente à privacidade dos dados que nos caracterizam, desde o nosso número de identificação nacional às nossas preferências de navegação na internet. Isto é resultado da divulgação de cada vez mais casos de roubo de dados virtuais ou do *input* que é retirado dos milhares de dados que produzimos diariamente.

A recolha massiva e o armazenamento total dos dados em variados sistemas informacionais, tem vindo a levantar diversas dúvidas relativamente ao fim desses dados – quer seja por quem e onde são armazenados, e para que objetivo. A discussão sobre o direito à privacidade tem-se intensificado nos últimos anos, em grande parte porque há quem considere que a privacidade se pode tornar obsoleta face ao novo uso social da internet. Segundo Capurro, Eldred & Nagel (2013), a privacidade não é uma propriedade das coisas, dos dados ou pessoas, mas sim uma atribuição dependente de um contexto social e cultural (o que não implica a existência de referencial de significação). Os autores mencionam também que quando existe uma transformação numa cultura, também a diferença entre privado e publico muda, e portanto a forma como a sociedade lida com essas duas formas também, já que ambas são um modo de *social being*.

A liberdade é um dos princípios centrais das democracias ocidentais, onde se inclui os EUA e parte da Europa. O livre movimento de pessoas, bens, serviços e capital na União Europeia, é representativo da aplicabilidade desse modelo. Num mundo globalizado e digital, o livre movimento e fluxo de informação dos dados sem restrições é (ou era) assumido como natural. Ainda que existia uma parte da informação que é

partilhada voluntariamente pelo individuo, como acontece nas redes sociais, outra parte é guardada e partilhada entre diferentes sistemas de informação, por vezes para fins diferentes para os quais foi recolhida e sem direta autorização do proprietário. Neste caso, refiro-me não apenas à informação privada, como também profissional e pública[59]. A entrada em vigor do RGPD, em Maio de 2018, reflete a execução prática das preocupações relativas à proteção de dados pessoais e privacidade dos cidadãos da União Europeia. Sendo que o RGPD cobre especificamente os membros da UE[60], e tendo em conta que até agora os dados fluíram livremente por todo o mundo, é pouco concreto o efeito a curto prazo nos dados de cidadãos europeus que circularam antes da efetivação do regulamento.

Embora exista um referencial de significação relativamente àquilo que é do foro pessoal ou público, é necessário ter em conta que a linha que divide a *privacidade* da *publicidade* é consideravelmente volátil, dependendo esta do contexto social e cultural em que a atribuição é dada. Ambos os conceitos representam modos de *social being* que têm vindo a ser cada vez mais estudados no âmbito da ética da informação muito devido ao crescimento do uso da internet e existe quem mesmo declare a privacidade como obsoleta no cibermundo (CAPURRO, ELDRED, & NAGEL, 2013). Neste contexto, a vigilância é feita com o recurso a dispositivos eletrónicos, redes de comunicação e de computadores, camaras de vigilância mas também com o auxílio de dispositivos acoplados a veículos aéreos não tripulados conhecidos como drones.

De acordo com o RGPD, a *integridade e confidencialidade* são princípios de tratamento de dados pessoais a serem cumpridos pelos responsáveis por estas atividades. A privacidade (em latim *privates* que significa *separado do resto*) é *"o direito de ser deixado sozinho […] o direito mais compreensivo e o mais valioso pelos homens civilizados"* (WARREN & BRANDEIS, 1890). De acordo com Calcutt (1990), privacidade é *"o direito do indivíduo em ser protegido face à intrusão à sua vida ou assuntos pessoais […] por meios físicos diretos ou pela publicação da informação".* Segundo a Constituição da República Portuguesa *"a todos são reconhecidos os direitos à identidade pessoal, ao*

[59] Tendo em conta a definição de Dados Pessoais da Comissão Europeia. Fonte: <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>.

[60] O RGPD é aplicável também aos seguintes países: Islândia, Liechtenstein e Noruega.

desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação." (Ponto 1 do art.º 26 Constituição da Republica Portuguesa[61]).

O artigo *The Right to Privacy* (1890) é reconhecido como a primeira publicação dos EUA a defender o direito à privacidade[62] mas apenas em 1934 é concretizado o Communications Act of 1934[63], que define o consenso social entre o governo, a indústria e os grupos de interesse relativamente ao papel dos recursos das comunicações e informação. Esta lei americana procurava restringir a habilidade de interceção secreta das comunicações pelo governo, todavia, de acordo com o estatuto federal de 1968, a interceção de comunicações via telefone ou telégrafo para propósito de espionagem ou vigilância era permitida por agentes de autoridade sob a obtenção de um mandato do tribunal (REYNOLDS, 2011).

Desde 1967, ao abrigo do *Freedom of Information Act* (FOIA) os cidadãos norte-americanos podem solicitar o acesso aos registos de qualquer agência federal, mediante indicação da finalidade de tratamento (p.e. uso comercial, pessoal ou cientifico). De acordo com o *website* oficial[64], esta lei é frequentemente reconhecida como "a lei que mantém os cidadãos informados acerca do seu governo" e uma "parte vital da democracia [norte-americana]". Sob o pedido desta autoridade, as agências são obrigadas a fornecer qualquer informação solicitada, salvo exceções de proteção de interesses como privacidade pessoal[65], segurança nacional e cumprimento da lei. O *Privacy Act of 1974*[66] estabelece um código de práticas de informação que limitam o tratamento de dados dos civis pelo Governo. Esta lei pretende salvaguardar os indivíduos da invasão de privacidade por agências federais[67], exceto a CIA (REYNOLDS, 2011). Em Portugal, a Constituição Portuguesa de 1976 menciona que "todos os

[61] Fonte: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

[62] Fonte: <http://www.igc.fd.uc.pt/manual/pdfs/L.pdf>.

[63] Em Português: *Lei Da Comunicações de 1934*. Apenas contempla os sistemas telefónicos, telegráficos e radiodifusão.

[64] Fonte: <https://www.foia.gov/faq.html>.

[65] Caso a informação diga respeito a terceiros

[66] Em Português: *Lei da Privacidade de 1974.*

[67] Fonte: <https://www.justice.gov/opcl/privacy-act-1974>.

cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei". Esta ideia é complementada pela definição de Caloyannides (2003) que diz privacidade é o "direito do indivíduo em controlar a recolha e uso da sua informação". O art.º 12 da Declaração Universal dos Direitos Humanos (DUDH) estabelece que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei". O Comité dos Direitos Humanos tem como função monitorizar o cumprimento das obrigações impostas pelo Pacto Internacional Sobre os Direitos Civis e Políticos (PIDCP), que desenvolve o conteúdo jurídico dos direitos da Declaração Universal dos Direitos Humanos. O art.º 17 do PIDCP garante o "direito à proteção da vida privada, família, domicílio e correspondência, honra e reputação" [68] e pode dividir-se em vários subgrupos como: privacidade; identidade; integridade; intimidade; autonomia; comunicação e sexualidade[29].

A *Organization for Economic Co-operation and Development* (OECD[69] estabelece, em conjunto com governos, *policy makers* e cidadãos, normas internacionais para dar resposta a desafios sociais, económicos e ambientais. As *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[70] (abreviadamente *OECD Privacy Framework*) constituem o primeiro acordo aceite internacionalmente (pelos países membros) no que diz respeitos princípios básicos de privacidade que deveriam ser aplicados nacionalmente. A primeira versão deste documento data 1980, tendo sofrido uma atualização em 2013 e bo presente ano está planeada uma revisão tendo em conta o ambiente digital em que vivemos. Entre 1980 e 2013, verifiquei que os princípios se mantiveram inalterados (pág. 14, parte II) e constatei uma correspondência com os princípios de proteção de dados do RGPD (art.º 5 do RGPD), os quais apresento de seguida.

[68] Fonte: <http://gddc.ministeriopublico.pt/faq/pacto-internacional-sobre-os-direitos-civis-e-politicos-pidcp-conteudo>.

[69] Da qual faz parte Portugal e os Estados Unidos da América. Fonte: <https://www.oecd.org/about/>.

[70] Abreviadamente conhecida como OECD *Privacy Framework*/ *Framework* de Privacidade da OECD. Fonte: <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

Figura 5 - Comparação entre o OECD Privacy Framework e o RGPD

Os princípios presentes em ambos os documentos são interligáveis e misturam-se entre si, desenvolvida de imediato:

- A *Limitação de Recolha* (1) diz que os dados devem ser obtidos de uma forma legal, o seu tratamento é apropriado e consentido. Isto é verificado pelo princípio (a) e (b).
- A *Qualidade dos Dados* (2) garante que os dados devem ser relevantes para o uso em questão e exatos, completos e atualizados (b).
- A *Especificação do Propósito* (3) indica uma recolha limitada ao cumprimento da finalidade para o qual os dados foram recolhidos (c), existindo por isso uma Limitação ao Uso (4) por consentimento ou autoridade legal. O princípio 4 também é indiretamente ligado com a Limitação da Conservação (d) considerando que os dados apenas são guardados durante o período necessário para o cumprimento daquela finalidade.

- A *Salvaguarda da Segurança* (5) contempla a proteção contra riscos, perdas, acesso não autorizado, destruição, utilização, modificação e divulgação dos dados, o que se encontra diretamente relacionado com o princípio (e).

Verifiquei não existir uma relação direta entre os princípios do RGPD, presentes no art.º 5, com os princípios (6), (7) e (8), contudo eles são relacionáveis com outros artigos do RGPD:

- A *Participação Individual* (6) refere-se, principalmente, aos direitos dos titulares de dados que são mencionados no RGPD do art.º 15 a 22 e no art.º 34. São estes: o direito de acesso aos dados; direito à retificação e apagamento (também chamado direito ao esquecimento); direito à limitação do tratamento; direito de portabilidade dos dados; direito de oposição; direito a não ficar sujeito a decisões individuais automatizadas; direito de reclamação e pedido de indemnização.
- A *Openess* (7) diz respeito à existência de uma política de transparência de práticas de tratamento de dados, prestando respeito aos dados pessoais. Esta informação está disponível no art.º 13 do RGPD.
- A *Responsabilidade* (8) tem em consideração o dever do encarregado/responsável pela proteção de dados em cumprir os princípios indicados, conforme art.º 39 do RGPD.

Reynolds (2010) refere que, enquanto conceito legal, o direito à privacidade compreende quatro aspetos:

- *Proteção contra intrusões não razoáveis sobre um indivíduo* (como a recolha de detalhes sobre os hábitos de navegação da Web de um indivíduo);
- *Proteção contra a apropriação de um nome ou imagem* (como roubo de identidade);
- *Proteção contra divulgação não razoável da vida privada do titular* (como a revelação de detalhes sobre a condição médica)

- *Proteção contra divulgação que, injustificadamente, crie uma imagem enganadora acerca do individuo* (como a publicação de informações falsas sobre alguém num *website*)

Para o âmbito desta investigação terá efeito a primeira dimensão indicada: *proteção contra intrusões não razoáveis sobre um individuo.* A razoabilidade é o foco e, como já foi descrito, esta poderá variar consoante princípios e valores, ainda que existam ordens e regulamentações mas que não possuem um caracter efetivo internacionalmente, como o Manual de Tallinn.

Ser vigilante significa "produzir inteligência sobre ameaças e estar ciente da situação para identificar padrões prejudiciais de comportamento"[71]. A evolução decorre da aquisição de conhecimento e uso da inteligência, sendo esta postura aplicável a diferentes circunstâncias e diferentes organizações. Vivemos numa sociedade em que queremos adquirir constantemente sempre mais dados, mais informação, mais conhecimento, mais inteligência. Por norma, o ser humano é competitivo e quantos mais recursos tiver à sua disposição, mesmo que estes nunca sejam utilizados, maior é a sensação de possível sucesso. O número e a exatidão de tecnologias dispara aumenta proporcionalmente, ano após ano, bem como a sua utilização sob o fundamento de cumprimento legal. Hoje em dias somos reconhecidos por sistemas de geolocalização, *softwares* de reconhecimento facial e camaras de vigilância/termais, sem qualquer pedido de consentimento, mesmo que não se verifique uma licitude clara. De acordo com Reynolds (2010), os agentes da autoridade afirmam que o sistema de vigilância não viola os direitos à privacidade e que esta prática não difere dos métodos tradicionais utilizados, como o policiamento presencial. É verdade que, por ter sido escrita há quase uma década, esta obra possa estar desatualizada, contudo, não posso deixar de comentar a realidade que foi apresentada pois certamente que o policiamento/reconhecimento de suspeitos presencial é muito menos eficaz (em termos de rapidez, eficácia e número de recursos utilizados) do que a vigilância com recurso a tecnologia.

[71] De acordo com a consultora Deloitte. Fonte: <https://www2.deloitte.com/cl/es/pages/risk/solutions/ciber-vigilancia.html>.

À partida, a ciberespionagem e a cibervigilância parecem dois conceitos muito semelhantes mas, a um nível mais profundo, são bastante diferentes. A espionagem envolve atividades de penetração dos Sistemas de Informação usados pelo inimigo para obtenção de informação residente ou transacionada nesses sistemas, pertencente a esfera económica; militar e política. Já a vigilância envolve a interceção de comunicações entre uma ou duas partes e frequentemente requer um processamento de uma grande quantidade através de algoritmos para atingir um determinado nível de conhecimento (BANKS, 2016). Para além disso, a espionagem é normalmente associada ao ambiente militar e a vigilância diz respeito a uma atividade a larga-escala, potencialmente afetando um grande número de pessoas[72].

De acordo com Banks (2016), a "recolha de inteligência […] invade as liberdades dos cidadãos para além das necessidades razoáveis do governo". Após a divulgação dos sistemas de vigilância massiva norte-americana, por Edward Snowden, os *media* começaram a despertar a curiosidade nos seus seguidores e a própria sociedade começou a questionar até que ponto os interesses dos governos se sobrepunham aos seus próprios interesses e direitos individuais. Este é um assunto sensível que envolve diferentes organismos de poder, com diferentes formas de atuação e objetivos nem sempre concretos, e é por vezes difícil justificar e criticar os contornos destes episódios. Nos EUA, a erosão do direito à privacidade foi resultado da implementação de políticas antiterrorismo após o 9/11, e esse *mindset* dissipou-se por diferentes países pois "os estados consideram que, pelo facto de o terrorismo ser uma questão global, a busca de terroristas não pode ser limitada pelas fronteiras nacionais" e exige cooperação e troca de informações [73]. As leis de privacidade, bem como a sua aplicabilidade prática, variam entre países. Para efeitos de comparação, é necessário compreender a realidade de cada um dos países em análise em termos de administração desta regulamentação. A consolidação desta informação encontra-se no capítulo seguinte.

[72] Fonte: <https://www.schneier.com/blog/archives/2014/05/espionage_vs_su.html>.

[73] I Congresso Roraimense de Direitos Humanos e Direito Internacional (Brasil, 2015). Fonte: <https://www.academia.edu/34277944/AS_DIVERSAS_FACES_DO_DIREITO_AO_DESENVOLVIMENTO_E_A_PERSPECTIVA_CULTURAL>.

VI. AS CIBERESTRATÉGIAS

O presente capítulo apresenta uma compreensão global das abordagens cibernéticas dos Estados Unidos, Rússia e Portugal, tendo em conta as seguintes dimensões: *contexto histórico, geográfico e político; segurança nacional; cooperação internacional;* e *legislação nacional para a privacidade e proteção dos dados.*

O *contexto histórico, geográfico e político* pretende informar o leitor acerca das circunstâncias relevantes e modeladoras do país em análise para que se emita um julgamento futuro menos limitado e mais consciente.

Segue-se uma descrição do modelo de *segurança nacional* e suas responsabilidades de cada organização envolvidas. As ciberestratégias envolvem, normalmente, um conjunto de agências governamentais e possivelmente privadas - dedicadas a diferentes temas como a segurança pública, indústria ou até mesmo educação - mas a coordenação e a responsabilidade recai sobre diferentes tipos de autoridades.

A *cooperação internacional* compreende as atividades que englobam múltiplas organizações internacionais que atuam neste domínio com recurso à parceria política.

Por fim, é apresentada a *legislação nacional para a privacidade e proteção dos dados* e, se possível, verificar se existe algum documento normativo que defina os limites éticos no tratamento da informação civil.

a) Estados Unidos da América

CONTEXTO HISTÓRICO, GEOGRÁFICO E POLÍTICO

Os Estados Unidos da América são um conjunto de 59 estados/territórios[74] que, apesar serem individuais e, de certa forma, autónomos legislativamente, operam sobre o comando do governo dos EUA, presidido por Donald Trump desde 2016.

O século XVIII marca o princípio dos Estados Unidos, quando treze colónias adquiriram independência da Grã-Bretanha. O fim da Guerra Civil Americana (1861-1865), o primeiro grande conflito interno entre os estados do norte e do sul, unificou e estabeleceu os Estados Unidos como um só país, todavia, a sistematização e uniformização da lei do país não foi imediata, tendo existindo vários ataques ao governo, acusado de opressão e corrupção.

Em 1917 os EUA, que até então tinham tomado a decisão de não participar na 1º Guerra Mundial por considerarem estar protegidos maritimamente contra possíveis ataques, são provocados pela Alemanha a entrar naquele que foi o primeiro confronto internacional, juntando-se aos Aliados (HARDACH, 1981). Também na 2º Guerra Mundial, os Estados Unidos adotaram inicialmente uma postura neutra, contudo, face ao ataque do Japão à base norte-americana de Pearl Harbor em 1941, que resultou na morte de 2000 indivíduos e perdas materiais como navios, decidiram avançar com as suas tropas.[75] Este conflito mundial terminou com o ataque dos Estados Unidos sobre duas cidades Japonesas: Hiroshima, onde existia um centro militar; e Nagasaki.[76] Tal como no ataque de Pearl Harbor, milhares de civis foram expostos à bomba atómica.[77]

Desde que tomou posse como o 45º Presidente dos Estados Unidos da América, Trump foi por vezes criticado em relação à sua atuação política, mais fervorosa e menos diplomática que o seu antecessor Barack Obama. As relações entre os EUA e a China, Coreia do Norte e Rússia sempre foram inconstantes, resultado do historial de conflitos entre os estados, porém, atualmente a postura política dos países em questão muda

[74] Fonte: <https://www.usa.gov/states-and-territories>.

[75] Fonte: <https://www.history.navy.mil/browse-by-topic/wars-conflicts-and-operations/world-war-ii/1941/pearl-harbor.html>.

[76] Fonte: <https://www.osti.gov/opennet/manhattan-project-history/Events/1945/hiroshima.html>.

[77] Para mais detalhe acerca da história dos EUA, consultar a cronologia disponível no *website* oficial. Fonte: <https://www.usa.gov/history>.

com uma rapidez visivelmente mais superior. Se por um lado, Putin e Trump admitem um esforço para corrigir as relações entre as duas superpotências de uma forma cordial, por outro estão constantemente a trocar acusações.

SEGURANÇA NACIONAL

Cerca de 35 anos após a unificação dos Estados Unidos, as leis federais (transversais a todos os estados) bem como de agências de segurança nacional e combate ao crime, eram inexistentes. Atores estatais de alto nível, como o presidente McKinley, foram atacados por civis defensores da justiça na sociedade industrial e apelavam a uma orientação e controlo do governo. Teddy Roosevelt e Charles J. Bonaparte foram os principais responsáveis pela estruturação de uma organização que investigasse os incumprimentos da lei, o conhecido *Federal Bureau of Investigation* (FBI). Com o aumento da onda de crime e corrução, foram recrutados outros investigadores, com diferentes perfis de análise e conhecedores de direitos civis. As primeiras investigações abordavam principalmente a fraude bancária, violação de direitos de autor e trabalho forçado em território nacional, todavia, não tardou para que o espectro geográfico se alargasse a outros países, iniciando-se com a investigação de contrabando pelo México. A guerra declarada à Alemanha em 1917 acelerou a aprovação das leis respeitantes à espionagem e sabotagem, atribuindo responsabilidade ao FBI como a autoridade contra espionagem. Atualmente, o FBI investiga e coordena possíveis ameaças dirigidas contra o país e dedica-se, entre outros, ao combate ao cibercrime e terrorismo. Outra das principais prioridades do FBI é proteger os Estados Unidos de espionagem e operações de inteligência estrangeira, sem não descuidar a proteção dos direitos civis.[78]

Embora independentes e com focos particulares, o *Department of Homeland Security* (DHS) e o *Department of Defense* (DOD) cooperam em situação de perigo iminente ou ataque, seja ele que tipo for, em prol da salvaguarda do país, todavia, o segundo, que coordena as forças militares[79] e a NSA, apresenta um papel mais determinante no tema da ciberguerra. Nesse âmbito, a NSA intervém e supervisiona em

[78] Fontes: <https://www.fbi.gov/history/brief-history> e <https://www.fbi.gov/about/mission>.

[79] Excepto Guarda Costeira.

tempo-real eventos virtuais, analisando padrões e combatendo ameaças cibernéticas, decodificando e compilando toda a informação recolhida, e que poderá ser partilhada com a rede de serviços inteligência com vista a uma eficaz implementação de ciberestratégias de defesa da segurança nacional. Para além de ser o *standard* na gestão do ciber-risco norte-americano, a NSA é também uma organização de referência internacional no que toca à promoção e partilha da educação da segurança informática, desde a criação de normas orientadoras de boas práticas, à formação de novos profissionais, passando pelas parcerias com organizações privadas, como empresas e academias de pesquisa, através da iniciativa *NSA's Technology Transfer Program*, que visa compartilhar novos desenvolvimentos tecnológicos, a fim de beneficiar ambas as partes[80].

Facilmente confundida com a NSA, a CIA opera como uma organização independente e tem um contacto mais próximo com o topo da estrutura política dos EUA. Foca-se igualmente na recolha e análise de informação significativa para o preenchimento detalhado de lacunas de inteligência que visam proteção do território nacional, mas, neste caso particular, a informação é proveniente de outros países ou atores não estatais. Face ao julgamento das conclusões de análise pelo Conselho de Segurança Nacional[81], e em última instância do Presidente, podem ser determinadas intervenções secretas[82]. Sucessora da Agência de Serviços Estratégicos, dedicada à coordenação das atividades de espionagem dos EUA durante a Segunda Guerra Mundial, a CIA foi criada estrategicamente para responder à necessidade identificada durante a Guerra Fria de consolidar toda a informação respeitante à segurança nacional e de ter um serviço que aconselhasse a tomada de decisão do Presidente na prevenção e mitigação de riscos. Por norma, a CIA é uma fonte independente de análise de informação, no entanto, para maximizar a qualidade da inteligência produzida, a colaboração com outras agências é permitida e incentivada.[83] Ambos os serviços de inteligência parecem completar-se, no enquanto, a NSA tem uma presença mais forte

[80] Fonte: <https://www.nsa.gov/what-we-do/cybersecurity/>.

[81] Inclui Presidente, o Vice-Presidente, a Secretária do Estado e o Secretário de Defesa.

[82] Fonte: <https://www.cia.gov/about-cia/cia-vision-mission-values>.

[83] Fonte: <https://www.cia.gov/about-cia>.

em “solo” norte-americano e a CIA caracteriza-se frequentemente extensão a territórios estrangeiros.

A constituição do Foreign Intelligence Surveillance Court em 1978 surgiu da necessidade de formar um órgão cuja finalidade fosse exercer a jurisdição sobre pedidos de vigilância eletrónica, busca física e outras formas de ações de investigação estrangeira.

Em 2017, foi assinada a Ordem Executiva 13800 que visa fortalecer a cibersegurança das redes federais e das infraestruturas críticas norte-americanas. Esta iniciativa surgiu para colmatar falhas de segurança de informação verificada nesses sistemas de rede, sejam eles públicos ou privados. Na atual Estratégia Nacional dos Estados Unidos[84], foram identificadas várias medidas futuras a adotar, entre as quais:

- Centralizar a gestão e supervisão dos sistemas de cibersegurança de agências governamentais no *DHS,* excluindo o DOD e os sistemas de *Intelligence Community.*
- Atualizar os estatutos de vigilância e cibercrime para melhorar as capacidades da aplicação da lei de forma a reunir legalmente a evidência de atividade criminosa necessária para sancionar os atacantes.
- Proteger e promover os direitos humanos no ciberespaço (nomeadamente de liberdade de expressão) em conjunto com a academia, indústria e sociedade civil.

COOPERAÇÃO INTERNACIONAL

Num mundo altamente interconectado, a cibersegurança requer a colaboração de estados aliados e parceiros - nacionais ou internacionais e públicos ou privados. A NATO foi um sistema de defesa coletivo através do qual os Estados Membros concordam com a defesa mútua em resposta a um ataque externo (art. 5º). Criado em 1949 para proteger a zona Norte Atlântica de uma possível expansão militar da União Soviética (WILKINSON, 2010), atualmente esta entidade é responsável pela gestão de crises através da assistência mútua entre aliados (estados e outras organizações) na prevenção, mitigação e recuperação de ciberataques. Até à data, dos 193 países do

[84] Fonte: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

mundo, 29 dos são membros da NATO, incluindo os Estados Unidos desde 1949, e sensivelmente 40 não-membros são parceiros na discussão pontual de matérias políticas e de segurança que trabalham com a NATO mas estes não participam na tomada de decisão como se fossem países membro[85]. A NATO compromete-se a uma resolução de conflitos diplomática, amigável e pacífica mas, nessa impossibilidade, esta organização tem o poder militar de intervir na segurança de um país: *"As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma, no exercício do direito de legítima defesa, individual ou coletiva, reconhecido pelo artigo 51.° da Carta das Nações Unidas, prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a ação que considerar necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte."* (Art.º 5 do Tratado do Atlântico Norte)[86]

De acordo com a vigente Estratégia de Cibersegurança, os Estados Unidos pretendem reforçar a cooperação internacional na investigação de ciberatividades maliciosas ao liderar um projeto de um sistema interoperável global de partilha de informação entre agências/organizações de autoridade.

LEGISLAÇÃO NACIONAL PARA A PRIVACIDADE E PROTEÇÃO DOS DADOS

De acordo com Raul (2017), o regime norte-americano da privacidade é indiscutivelmente o mais antigo, mais robusto e bem desenvolvido. O sistema segue particularmente o princípio da reação a episódios de violação da privacidade, em vez da precaução como na União Europeia. Não obstante, a lei federal prevê restrições e proibições às comunicações eletrónicas, entre elas as quais:

[85] Fonte: <https://www.nato.int/nato-welcome/index.html>.

[86] Fonte: <https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt>.

Legislação e Normas relativas à Privacidade e Proteção de Dados nos Estados Unidos:
Constituição dos Estados Unidos da América
United States Bill of Rights (emendas à Constituição)
Foreign Intelligence Surveillance Act (FISA)
USA Freedom Act of 2015
Electronic Communications Privacy Act (EPCA)

Tabela 9 - Legislação e Normas de Privacidade e Proteção de Dados nos Estados Unidos

A proteção legal da privacidade dos civis é reconhecida na lei dos EUA desde 1890, inicialmente orientada para o setor comercial e atualmente alargada a tudo o que envolve a vida quotidiana. Alinhado com as diretrizes europeias, também os EUA dão importância à proteção da dignidade, autonomia e propriedade dos civis no mundo digital, estando previstas restrições e proibições legais do tratamento de dados para determinados tipos de setores como o financeiro e de saúde. O *Children's Online Privacy Protection Act* (COPPA) dedica-se a impor severos limites ao tratamento de dados de menores de 13 anos[87] por empresas, à semelhança como é exigido pelo RGPD e consequentemente em Portugal.[88]

Para controlo e restrição da intromissão do governo no direito à privacidade, foram realizadas emendas à Constituição dos Estados Unidos, a lei suprema nacional criada em 1787, de forma a prever as questões de privacidade, destacando-se a Quarta Emenda que proíbe a investigação irrazoável e define critérios para a emissão de mandatos para a instalação de escutas (ZIMAN, 2018). Esta emenda, aprovada em 1791, considera a busca legal para fins de detenção legal e se houver uma causa provável de busca sem mandado, justificada por perigo ou fuga iminente. Se verificada uma violação da quarta emenda por parte de funcionários federais, pode ser apresentada uma ação

[87] Fonte: <https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5#se16.1.312_18>.

[88] Fonte: <https://observador.pt/2019/06/14/portugal-aprova-lei-de-protecao-de-dados-um-ano-depois-do-rgpd/>.

bivens contra os agentes da lei federal por danos, resultantes de uma investigação e apreensão ilegal.[89]

No mundo digital, a Quarta Emenda da Constituição dos Estados Unidos da América aplica-se à investigação e apreensão de dispositivos eletrónicos. Em resposta aos ataques terroristas de 11 de setembro de 2001 ao World Trade Center e ao Pentágono, a legislação foi promulgada para, entre outros aspetos, reduzir legalmente as restrições de recolha de informações pelas agências norte-americanas sem autorização judicial, através do *US Patriot Act*[90] assinado pelo presidente George W. Bush. A secção 202 deste decreto confere permissão e autoridade para intercetar comunicações - orais ou eletrónicas - relacionadas com o terrorismo, contudo, a esfera que diz respeito ao terrorismo foi alargada ao território nacional, fruto do clima de desconfiança e suspeita que se instalou após os ataques. Cidadãos norte americanos ou estrangeiros, civis ou membros do governo, todos eram possíveis suspeitos. O *US Patriot Act* foi interpretado como uma resposta positiva à proteção nacional e, por essa essa razão, prorrogado pelo presidente Obama até 2015. Verificada a necessidade de balancear e adaptar as questões de segurança e privacidade, em particular pelo escândalo Snowden, o *US Patriot Act* foi substituído pelo *USA Freedom Act* nesse mesmo ano. Este documento legislativo voltava a limitar o uso da tecnologia e recolha de informação dos cidadãos pelas agências (LATIMER, 2018).

No seguimento da Diretiva Política Presidencial 41 (2016)[91], Morgan (2019) interpreta-a destacando que a proteção à privacidade dos cidadãos está dependente da identificação de um risco para a segurança nacional, ou seja, a salvaguarda dos dados dos civis pode ser desconsiderada se interferirem com os interesses governamentais. A crítica do autor é pertinente considerando que não existe uma atribuição sistemática e pragmática para definir a partir de que intensidade de risco supera o comprometimento deste direito.

O governo norte-americano foi criticado e acusado de recolha de informação dos cidadãos excessiva e desnecessária para propósitos de produção de inteligência para

[89] Fonte: <https://www.law.cornell.edu/wex/fourth_amendment>.

[90] Fonte: <https://www.congress.gov/107/bills/hr3162/BILLS-107hr3162enr.pdf>.

[91] A Diretiva Política Presidencial 41propõe ações para a melhoria da coordenação entre o setor privado e o governo na gestão de ciberataques.

segurança nacional. Durante décadas, o secretismo característico do trabalho das agências norte-americanas provocou curiosidade em Hollywood e deu lugar à exploração e preenchimento ficcional das lacunas existentes acerca do modo de operação destas organizações. Entre os inúmeros factos desmistificados, a CIA esclarece publicamente uma das crenças mais controversos - a espionagem de cidadãos norte-americanos: *"(…) Por orientação do presidente na Ordem Executiva 12333 de 1981, e de acordo com os procedimentos aprovados pelo Procurador-Geral, a CIA é restrita na recolha de informações de inteligência dirigidas contra cidadãos americanos. A recolha é permitida apenas para fins de inteligência autorizada; por exemplo, se houver uma razão para acreditar que um indivíduo está envolvido em espionagem ou atividades terroristas internacionais. Os procedimentos da CIA requerem aprovação superior para qualquer recolha que seja permitida e, dependendo da técnica de recolha utilizada, a sanção do Diretor de Inteligência Nacional e Procurador-Geral pode ser necessária. Essas restrições estão em vigor desde a década de 1970."*[92]

A agência acrescenta referindo que, na execução de uma missão internacional, são tomadas medidas preventivas para salvaguardar as informações recolhidas durante a operação que dizem respeito aos cidadãos americanos. Na CIA, o equilíbrio entre a necessidade de sigilo da organização e as questões de transparência, privacidade e liberdade civil é orientado pelo *Office of Privacy and Civil Liberties* (OPCL)[93] da CIA que confere a integridade na conduta das missões e garante os direitos dos americanos previstos pela lei federal. Possivelmente fruto do debate mediático, ético e até mesmo legal acerca da vigia do governo sob os seus cidadãos, as manifestações públicas de compromisso de proteção da liberdade civil nas organizações têm sido cada vez mais frequentes em agências americanos. Esta mudança cultural na CIA foi demonstrada através da publicação integral e pública, em 2017, das Diretrizes Gerais da Procuradoria da CIA[94], anexando um documento narrativo[95] detalhado orientador para os civis.

---

[92] Fonte: <https://www.cia.gov/news-information/featured-story-archive/2018-featured-story-archive/top-10-cia-myths.html>.

[93] Todas as agências federais incluem na sua estrutura gabinetes de privacidade, contudo, a determinados departamentos e agências – particularmente a CIA, NSA e o FBI – é obrigatória por lei a existência desta repartição administrativa.

[94] Fonte: <https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf>.

[95] Fonte: <https://www.cia.gov/about-cia/privacy-and-civil-liberties/Detailed-Overview-CIA-AG-Guidelines.pdf>.

Em 2013, aquando da reforço dos programas de inteligência da NSA, o ex-presidente Barack Obama anunciou diversas iniciativas que intencionavam o aumento da confiança dos civis nos programas, entre as quais a centralização de responsabilidades e serviços de consultoria num departamento dedicado totalmente à privacidade e proteção dos dados dos americanos - o *NSA Civil Liberties and Privacy Office*. Tal como a CIA, a transparência apropriada e significativa, bem como a salvaguarda da liberdade e privacidade civil, é mencionada como parte integrante do planeamento e execução das operações da NSA. Para esclarecer a FISA, o governo publicou um documento [96] que orienta e limita o ato de vigilância internacional, indicando que, o Governo dos Estados Unidos da América não pode obter informação dos servidores dos prestadores de serviços de comunicações eletrónicas sem aprovação prévia da FISA. Adicionalmente, é esclarecido que a vigia de um individuo só é permitida em situação de prevenção de terrorismo, ciberatividades hostis ou proliferação nuclear, e sempre mediante aprovação do tribunal. Para além disso, para que esta atividade seja considerada legal, o alvo:

- Não pode ser um cidadão norte-americano ou qualquer pessoa que se encontre nos Estados Unidos
- Não pode ser um cidadão estrangeiro se o propósito é adquirir informação de um individuo que se encontre nos Estados Unidos

[96] Fonte: <https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf>.

b) Rússia

CONTEXTO HISTÓRICO, GEOGRÁFICO E POLÍTICO

Constituída oficialmente como Federação Russa, a Rússia é a região com uma data de estabelecimento mais recente, nos moldes como a conhecemos hoje, quando comparada à formação dos Estados Unidos e União Europeia. A formação da civilização russa remonta às tribos eslavas que instalaram no território ao qual hoje damos o nome de Kiev e que, ao longo dos séculos seguintes, os seus sucessores começaram a ocupar outros territórios, divulgando a fé cristã. Séculos se passaram e depois de muitas invasões e expulsão de outros povos, em 1886 o território russo ocupava parte da europa e toda a parte norte da Ásia. Devido à sua extensão territorial, mesmo a atual, nunca foi consensual se os russos são europeus, asiáticos ou euroasiáticos.

Estabelecida como monarquia nacional centralizada em 1546, a unificação da civilização russa aconteceu sob a autoridade e moderação do primeiro czar russo Ivan IV, o Terrível. Foi também nesta altura que surgiu a primeira força de investigação secreta que perseguia e torturava qualquer pessoa considerada como possível inimiga ao governo. Durante séculos, a Rússia esteve envolvida em conflitos, algumas vezes aliada a outros países e outras completamente independentes, o que fragilizou a sua estrutura administrativa e económica do país. A erupção da Primeira Guerra Mundial, seguida pela anulação e substituição da Monarquia pelo Estado Socialista, originou um conflito nacional a larga escala. A Guerra Civil Russa de 1917 foi um período difícil pela perda de diversos territórios e clima de revolta dos civis, mas este episódio transformou-se numa oportunidade de reformar e centralizar politicamente o país com a formação da União das Repúblicas Socialistas Soviéticas (abreviadamente União Soviética ou URSS).

Durante a Segunda Guerra Mundial, foi assinado entre a URSS e a Alemanha um pacto nazi-soviético de tréguas, quebrado pouco depois pelo governo liderado por Adolf Hitler. Por essa razão, a Rússia junta-se aos Aliados, iniciando-se a relação de colaboração com os EUA. Sem embargo, fora deste contexto, a Rússia e os Estados Unidos eram (e são) duas das maiores superpotências políticas e económicas da história e, por conseguinte, diretas adversárias na conquista internacional. Um dos grandes marcos da relação entre os Estados Unidos da América e a Rússia, naquela altura parte

da União das Repúblicas Socialistas Soviéticas, foi o acordo temporário pós Guerra Fria entre os dois países relativamente à divisão da Coreia, em que a URSS controlaria a parte norte e os EUA a parte sul, enquanto não era eleito um responsável que unificasse o país. Todavia, a União Soviética boicotou o acordo em 1950 ao ter apoiado, em conjunto com a China, a invasão da Coreia do Norte sobre a Coreia do Sul. Se a o governo da Coreia estava dividido entre as superpotências, a Guerra Coreana mascarava de certa forma o conflito entre as duas superpotências (WEATHERSBY, 1993).

A crise económica e política debilitou o governo comunista e dissolveu a URSS em 15 estados independentes. A república constituinte da União Soviética diminuiu a sua extensão territorial mas continua a ser o país como mais espaço geográfico no planeta e é um dos principais atores intervenientes do ciberespaço.

Atualmente, na Rússia, as relações internacionais são da responsabilidade do Presidente Vladimir Putin (Constituição da Rússia[97], art.º 80), que, por sua vez, é um ex-agente da KGB1. Em 1991, posteriormente à dissolução da URSS, a Federação Russa assumiu a dívida do estado socialista bem como herdou o seu exército (AUSTIN & MURAVIEV, 2000) e, por ser a maior das repúblicas dessa divisão, é vulgarmente considerada o estado sucessor da União Soviética. Ainda assim, para fins deste estudo, irei considerar a informação relativa à União Soviética, tendo em conta que a memória histórica poderá afetar as relações modernas e poderá ser decisivo para o meu estudo.

SEGURANÇA NACIONAL

A Rússia sempre teve consciência do valor da informação para a segurança nacional. O *Komitet Gosudarstvennoy Bezopasnosti* (KGB) foi a principal agência com afiliação militar dedicada à produção de inteligência para efeitos de segurança interna. Aquando do início do desmantelamento da KGB, a Rússia formou uma agência separada, a *Federal'noe Agentstvo Pravitelstvennoi Svyazi I Informatsii* (FASPSI), dedicada apenas às questões de segurança da informação nomeadamente relacionadas com comunicações governamentais. Em 2013, a FASPSI acabou por ser incorporada subunidade estrutural no *Federalnaya Sluzhba Okhrany* (FSO).

[97] Constituição da Federação Russa disponível em: <http://constitution.kremlin.ru/>, consultada a 04/06/2019.

Com a dissolução total definitiva da URSS, o KGB decompôs-se em duas agências que operam até aos dias de hoje: o *Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* (FSB) e o *Sluzhba Vneshney Razvedki* (SVR). O FSB é um serviço militar que atua com as forças armadas russas e a maior parte das atividades de segurança do país estão à sua responsabilidade, exceto a espionagem que é executada pelo SVR mas que em último caso poderá ser orientada pelo FSB (SAKWA, 2008).

De acordo com Connel & Vogler (2017), o ciberespaço foi durante muitos anos um domínio exclusivo dos serviços de segurança. As ciberoperações – tanto ofensivas como defensivas - têm vindo a ganhar particular destaque nas estratégias militares russas em matéria de proteção nacional. Entre outras táticas, encontra-se a formação da Diretoria K, um órgão administrativo do Ministério da Administração Interna que tem como principal atividades o combate ao crime no domínio do ciberespaço, como o acesso ilegal à informação e violação de direitos relacionados com as tecnologias de informação. O Ministério da Administração Interna interage ativamente com os organismos internacionais regularizadoras e mitigadoras de conflitos internacionais.

COOPERAÇÃO INTERNACIONAL

À semelhança de outros estados da ex-URSS, também a Rússia não é um membro integrante da União Europeia, facilmente justificado por questões económicas, geográficas e/ou políticas.

Tal como os Estados Unidos, a URSS foi um dos 51 membros fundadores da Organização das Nações Unidas (ONU)[98], um órgão internacional que tem como principal propósito manter a paz e segurança no mundo através da promoção da cooperação entre países na solução de problemas ligados com a violação de direitos humanos.

O programa *Partnership for Peace* é um acordo entre a NATO e países não membros da organização (entre os quais aqueles que compunham a URSS), de forma individual, para a cooperação e reforço da paz internacional. Estabelecido em 1994 após a proposta dos Estados Unidos, o programa permite aos participantes desenvolver uma relação individual e definir prioridades bem como os contornos da relação. Este acordo não

[98] Fonte: <https://www.un.org/en/member-state>.

limita totalmente a liberdade de movimento político do país parceiro mas facilita a gestão da paz mundial pela NATO, o que é benéfico para as duas partes.[99] Em consequência da intensificação dos conflitos do médio oriente, os Estados Unidos, Rússia e Portugal[100] são alguns dos participantes do Quarteto de Madrid que promove o processo de paz no conflito árabe-israelense.

Ao longo da última década, foi identificada uma multiplicidade de variantes de *ransomware*[101] em diversas plataformas que provocaram um impacto negativo nos sistemas de informação. Em 2012 surge uma nova expressão deste crime - o *ransomware* governamental – que, através de técnicas de engenharia social, notifica a vítima, em nome de agências de autoridade (p.e. FBI, Interpol), que esta incorreu de um crime e era exigido o pagamento de uma coima.

Figura 6 - Exemplo de um ataque de *ransomware*[102]

[99] Fonte: <https://www.nato.int/cps/ra/natohq/topics_50349.htm>.

[100] O Quarteto de Madrid inclui duas instituições (a União Europeia e a ONU) e dois países, a Rússia e os EUA.

[101] *Malware* que restringe o acesso do utilizador ao sistema infetado presente em computadores e dispositivos digitais. O desbloqueio ou decifragem do sistema é feito em troca de um pagamento de resgate.

[102] Fonte: <https://www.nomoreransom.org/pt/ransomware-qa.html>

Via Ministério da Administração Interna, a Rússia apoia a iniciativa *No More Ransom* ao abrigo da Europol. Lançado em 2016, este projeto visa sensibilizar, educar, orientar e ajudar vítimas ou potenciais vítimas destes ataques. Portugal também é parceiro neste projeto, todavia, não se verificou uma relação, pelo menos direta, entre esta iniciativa e os EUA.

LEGISLAÇÃO NACIONAL PARA A PRIVACIDADE E PROTEÇÃO DOS DADOS

O governo russo tem vindo a tomar medidas adicionas para proteger os dados dos seus cidadãos principalmente através destes dois documentos com carácter legislativo:

Legislação e Normas relativas à Privacidade e Proteção de Dados na Rússia:
Constituição da Federação Russa
Lei Federal nº152-FZ

Tabela 10 - Legislação e Normas de Privacidade e Proteção de Dados na Rússia

A sucessora da URSS rege-se pela Constituição da Federação Russa, adotada por voto popular em 12 de Dezembro de 1993. A Constituição garante que "o reconhecimento […] e a proteção dos direitos e liberdades de uma pessoa e de um cidadão é um dever do Estado" (art.º 2) e que "as formas de propriedade privada, estatal, municipal e outras são igualmente reconhecidas e protegidas" (art.º 9). A segunda seção do documento é dedicado aos direitos e liberdades do homem e do cidadão e refere que "todos os indivíduos têm direito à privacidade [incluindo o] direito à confidencialidade de correspondência, conversas telefónicas […] e outras comunicações", sendo a recolha, armazenamento, uso e disseminação de informações sobre a vida privada de uma pessoa apenas permitida apenas com o consentimento do titular dos dados (art.º 23 e 24). Como em qualquer constituição, para fins de proteção

nacional são previstas restrição deste direito[103], permitida apenas com base numa decisão judicial, à exceção da privacidade da vida pessoal e familiar.

O Roskomnadzor, como é abreviadamente nomeado, é o serviço federal de supervisão e regulação das tecnologias de informação, comunicações e media para proteger os direitos de proteção de dados pessoais. Este foi o primeiro organismo autorizado a executar exclusivamente a supervisão estatal nesta matéria. Nos termos do art.º 22 e a seção 4 do art.º 25 da Lei Federal nº 152-FZ de 27 de julho de 2006[104], os operadores são obrigados a notificar esta autoridade de controlo sobre a sua intenção de processar dados pessoais antes do tratamento.

[103] "Em estado de emergência, a fim de garantir a segurança dos cidadãos e proteger a ordem constitucional, de acordo com o direito constitucional federal, podem ser estabelecidas certas restrições aos direitos e liberdades, indicando os limites e a duração da sua validade." (art.º 56 da Constituição da Federação Russa)

[104] Lei Federal nº 152-FZ de 27 de julho de 2006. Fonte: <https://pd.rkn.gov.ru/authority/p146/p164/>.

c) Portugal

CONTEXTO HISTÓRICO, GEOGRÁFICO E POLÍTICO

Situado na Península Ibérica, Portugal é um país que conta com milhares de anos de descobrimentos e conquistas internacionais mas também de ocupação do seu território por celtas, lusitanos, romanos, mouros e mais tarde dos espanhóis. Durante vários anos, diversas tentativas foram feitas para alcançar a desassociação e independência do poder castelhano, efetivada no século XVII. O regime monárquico português que durava há cerca de oito séculos cai e é substituída pela República Portuguesa em 1910. Sob o regime republicano, Portugal lutou na Primeira Guerra Mundial ao lado das principais potências associadas como os Estados Unidos e Rússia. Em 1939, Portugal encontrava-se sob o regime ditatorial do Estado Novo[105] e declarou neutralidade, durante a Segunda Guerra Mundial, tal como Espanha, cumprindo-a durante todo o período. Esta isenção provia o estado português de autonomia e liberdade de movimento político para tomar as suas próprias decisões.[106]

Atualmente, Portugal é um estado democrático semipresidencialista, presidido por Marcelo Rebelo de Sousa e governado pelo primeiro-ministro António Costa.[107] Contrariamente à Rússia e aos Estados Unidos, Portugal é subdividido geograficamente em 18 distritos em Portugal Continental sem autonomia de governo próprio e por 2 regiões autónomas, os Arquipélagos dos Açores e da Madeira[108]. Naturalmente, os episódios de invasão e expansão do território português foram decisivos para moldar as relações internacionais de Portugal como o resto do mundo. As repercussões das ações portuguesas dificilmente se sentem agora, possivelmente porque, ao contrário dos outros dois países em estudo, Portugal não é uma ameaça económica, política e tecnológica, mas sim visto como um possível país parceiro.

---

[105] Governado por António de Oliveira Salazar, considerada com uma das figuras mais polémicas da política portuguesa.

[106] Fonte: < https://www.portaldiplomatico.mne.gov.pt/sobre-portugal>

[107] A composição do Governo está disponível em: <https://www.portugal.gov.pt/pt/gc21/governo/composicao>.

[108] O Governo é representado nas Regiões Autónomas por um Representante da República, cuja nomeação é da responsabilidade exclusiva do Presidente da República.

SEGURANÇA NACIONAL

Em substituição do Instituto de Altos Estudos da Defesa Nacional (IAEDN), o Instituto de Defesa Nacional (IDN) é criado em 1976 pelo Decreto-Lei 550-D/76 como a primeira organização portuguesa a dedicar-se ao estudo, investigação e divulgação da problemática da Defesa Nacional. É parte integrante do Ministério da Defesa Nacional mas dispõe de autonomia científica, pedagógica e administrativa[109]. Tem como principal missão o apoio à formulação do pensamento estratégico nacional através do estudo, investigação e divulgação de informação relativa à segurança nacional.

O reconhecimento da necessidade de um sistema de informações específico, dedicado à proteção nacional, foi motivado pelos atentados às embaixadas de Israel e Turquia em território português (1979-1983). Em resultado, a Lei nº 30/84 estabelece a criação de um Sistema de Informações da República Portuguesa (SIRP) que contempla atualmente dois serviços subordinados[110] e até 2004 tutelados pelo Ministério da Defesa Nacional e Ministério da Administração Interna:

- Serviço de Informações Estratégicas de Defesa (SIED)
- Serviço de Informações de Segurança (SIS)

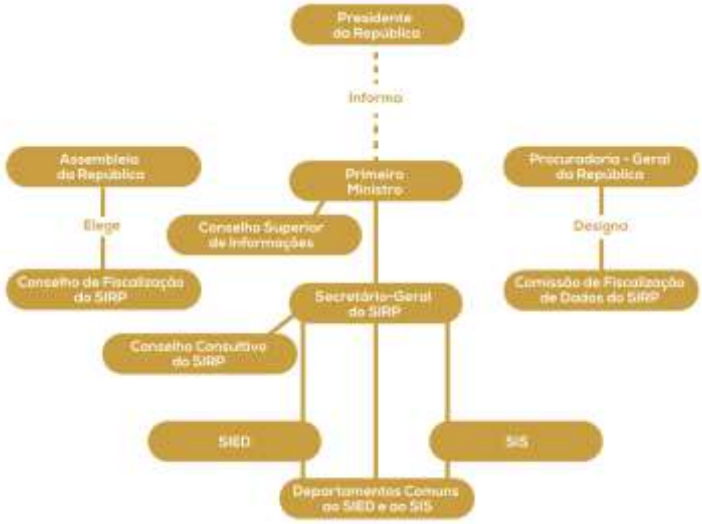

Figura 7 - Organograma e Estrutura, cf. SIRP[111]

[109] Fonte: <https://www.idn.gov.pt/index.php?mod=001&area=060>.

[110] De acordo com a cronologia disponibilizada pelo SIED, de 1984 a 1995 existia um terceiro serviço dedicado ao Serviço de Informações Militares (SIM) mas que foi absorvido pelo SIED. Fonte: <https://www.sied.pt/quem-somos/historia>.

[111] Fonte: <https://www.sirp.pt/quem-somos/organograma-e-estrutura>.

Para o cumprimento das respetivas missões, é verificado o dever legal de "acionar todos os meios técnicos e humanos (...) para a recolha e tratamento de informações", desde que em conformidade com a legislação em vigor; respeitando o limite dos direitos, liberdades e garantias fundamentais dos cidadãos, tal como consagrados na Constituição da República Portuguesa. Adicionalmente, não é permitido ao SIS a realização de interceção de comunicações e a detenção de pessoas ou a instrução de inquéritos ou processos penais ou qualquer outra atividade da competência de outras autoridades não é autorizada.

Aos agentes e funcionários desta organização recaem deveres particulares como o dever de sigilo e atividade em regime de exclusividade e total disponibilidade bem como a possibilidade de adoção de uma identidade alternativa, caso a missão assim o exija. Vulgarmente nomeados como Serviços Secretos Portugueses, o SIED e o SIS "trabalha[m] em segredo (de forma a alcançar os seus fins) mas não são secretos"[112], sendo que se confirma a transparência obrigatória requerida para duas organizações: quem são, onde atuam; que missão têm e como são reguladas.

O SIS executa as suas missões de acordo com os princípios de necessidade; proporcionalidade e adequação, sendo os dados recolhidos por[113]:

- Fontes abertas e documentos não classificados disponíveis ao público geral (Open Source Intelligence – OSINT)
- Fontes humanas (Human Intelligence – HUMINT)
- Outras entidades públicas (mediante a celebração de um protocolo)

Na sessão de abertura do 1º Painel do V Seminário sobre "Ameaças Assimétricas e Planeamento Estratégico"[114], realizado em 2017 na Reitoria da Universidade Nova de Lisboa, o diretor do SIS, Adélio Neiva da Cruz, refere que a proteção do espaço geográfico é ainda muito importante e representante da sobrevivência e poder nacional - daí não existir uma dedicação exclusiva destas organizações no tratamento de informações que fluem no ciberespaço - todavia, o carácter imprevisto e inesperado das novas ameaças desafia os modelo de operação dos Serviços de Informação e não deverá ser desvalorizado.

[112] Fonte: <https://www.sied.pt/quem-somos/faqs#collapseSixteen>.

[113] Fonte: <https://www.sis.pt/quem-somos/o-sis>.

[114] Fonte: <https://www.sirp.pt/media/2018/10/ameacas-assimetricas-e-planeamento-estrategico.pdf>.

Em matéria de cibersegurança, os objetivos da Comissão Europeia passam por dotar os países membro de capacidades de cibersegurança, promover a cooperação e desenvolver políticas unificadas.[115] Em concordância com as diretivas europeias e acompanhando a necessidade de conceber uma organização responsável pelo plano estratégico nacional para o ciberespaço, surgiu o Centro Nacional de Cibersegurança (CNCS) sob a alçada do Gabinete Nacional de Segurança (GNS).

O CERT.PT[116] é um serviço integrante do CNCS que "gere a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de infraestruturas críticas[117] e prestadores de serviços digitais" e promove ações de formação, exercícios nacionais e definição de um conjunto mínimo de capacidades técnicas, operacionais e humanos para técnicos e decisores que operem num CSIRT[118],

É atribuída competência ao Tribunal Constitucional para interpretar a Constituição e fiscalizar a conformidade das leis com as suas disposições; executando ações judiciais se se validar violações da Constituição.

Portugal não teve um papel particularmente relevante em nenhum conflito internacional que envolvesse o ciberespaço. Não obstante, a proteção do ciberespaço é uma das prioridades portuguesas, tendo sido publicada recentemente a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 que assenta no princípio da subsidiariedade, da complementaridade e da proporcionalidade. Tal como as suas antecessoras, esta estratégia "funda–se no compromisso de aprofundar a segurança das redes e sistemas de informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas" e "assenta no direito vigente que regula as relações internacionais soberanas, designadamente na Carta das Nações Unidas e no Direito Internacional Humanitário [e] na política de ciberdefesa da NATO […]"[119]. Esta estratégia tem, entre

[115] Fonte: <https://www.cncs.gov.pt/cooperacao/comissao-europeia/>.

[116] A sigla CERT corresponde ao seu nome em inglês *Community Emergency Response Team*. Mais informações disponível em: <https://www.cncs.gov.pt/certpt/>.

[117] Sectores de infraestruturas críticas: energia – como eletricidade, petróleo e gás - e transportes - rodoviários; ferroviários; aéreos e marítimos.

[118] Sigla para *Computer Security Incident Response Team*.

[119] Resolução do Conselho de Ministros n.º 92/2019.

outras, as seguintes missões: aprofundar o emprego dual e cooperativo das forças armadas e das organizações de cibersegurança, que demonstra ser o método mais eficaz de segurança nacional ao ciberespaço; incrementar a interoperabilidade das estruturas e, no domínio da atuação internacional; e desenvolver a disciplina de ciberdiplomacia[120].

COOPERAÇÃO INTERNACIONAL

Atualmente são 28 os países membros da UE, uma união económica e política que tem como principal objetivo promover variados valores, como a democracia, liberdade e proteção dos direitos humanos – nomeadamente através da Carta dos Direitos Fundamentais da União Europeia, "onde se consagra o direito à proteção de dados pessoais". A projeção de uma parceria inter-estado surgiu após a 2º Guerra Mundial, supondo-se que se existisse uma dependência comercial entre os 6 países aderentes, diminuir-se-ia a probabilidade de conflito. A relação acabou por evoluir, tendo sido extensível a outros temas, como ambiente, saúde, relações externas e segurança, como a outros países.[121] As questões e preocupações militares não eram o principal foco da EU, tendo em conta que estas cabiam principalmente à NATO.

A participação na NATO está aberta à "qualquer estado europeu em posição de aprofundar os princípios deste Tratado e contribuir para a segurança da área do Atlântico Norte".[122] É determinante referir que nem todos os estados da União Europeia são membros integrantes da NATO – como é o caso da Áustria - e vice-versa – como a Turquia. O regime ditatorial salazarista não impediu a integração de Portugal na NATO aquando da sua fundação, em 1949, mas a adesão de Espanha, que também vivia uma ditadura, foi recusada. Em declarações à Lusa, Daniel Marcos, historiador do Instituto de Políticas e Relações Internacionais declara que "Portugal foi convidado a integrar a NATO pela importância estratégica da base das Lajes […] para os norte-americanos", uma resposta direta aos interesses de terceiros, mesmo que possa ter provado o sentimento de uma aceitação e legitimação internacional do regime salazarista[123]. À

[120] Disciplina de ação externa para o estabelecimento das relações pacíficas entre estados.

[121] Os 28 Estados-Membros da União Europeia, disponível em: <https://europa.eu/european-union/about-eu/countries_pt#28members>, consultado a 04/06/2019.

[122] https://www.nato.int/nato-welcome/index.html

[123] https://www.publico.pt/2019/04/02/politica/noticia/nato-crucial-portugal-durante-ditadura-tambem-democracia-1867662

semelhança dos EUA e da Rússia, Portugal é membro da Organização para a Segurança e Cooperação na Europa (OSCE). Os EUA e Portugal participaram no processo de formação da OSCE e fazem parte grupo original de países signatários da Ata de Helsínquia.

A cooperação internacional também contempla a partilha de conhecimento e verifica-se muitos esforços para a partilha de informação entre estados sobre estas matérias. O *Information Sharing and Analysis Center* (ISAC) opera uma dessas plataformas colaborativas de centralização da informação e incentivam a troca de conhecimento e experiências entre entidades públicas e privadas relativas.

LEGISLAÇÃO NACIONAL PARA A PRIVACIDADE E PROTEÇÃO DOS DADOS

Criada em 1991, a Comissão Nacional de Proteção de Dados (CNPD) é a entidade administrativa independente com poder de exercício de autoridade no controlo e fiscalização do processamento de dados pessoais, "em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei"[124]. Com a implementação do Regulamento Geral de Proteção de Dados na Europa, a privacidade dos dados tornou-se uma das maiores prioridades nacionais e uma preocupação a considerar pelos sectores públicos e privados. De acordo com a CNPD, a *framework* legal de proteção de dados é regulada por: [125]

Legislação e Normas relativas à Privacidade e Proteção de Dados em Portugal:
Artª 35 da Constituição Portuguesa – Utilização da Informática
Lei 67/68 – Lei da Proteção de Dados Pessoais
Lei 103/2015 – adita o artº 45 - A - A Inserção de dados falsos - à Lei 67/98
Lei 2/ 94 – estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen
Lei 36/ 2003 – Regula o estatuto e competências do membro nacional da EUROJUST
Lei 43/ 2004 – Lei da organização e funcionamento da CNPD

Tabela 11 - Legislação e Normas de Privacidade e Proteção de Dados em Portugal

[124] Fonte: <https://www.cnpd.pt/bin/cnpd/acnpd.htm>.

[125] Fonte: <https://www.cnpd.pt/bin/legis/leis_nacional.htm#protecao_de_Dados_Pessoais>.

Existem regulações específicas para determinados sectores como saúde, comunicações eletrónicas e trabalho. Em seguida é referida a legislação da videovigilância:

Legislação e Normas relativas à Videovigilância em Portugal:
Lei 1/ 2005 – regula a videovigilância pelas forças de segurança em locais públicos de utilização comum
Decreto-Lei 207/ 2005 - Regula os meios de vigilância Eletrónica rodoviária utilizados pelas forças de segurança
Lei 51/ 2006 – regula a utilização de sistemas de vigilância rodoviária pela EP e pelas concessionárias rodoviárias
Lei 33/ 2007 – regula a instalação e utilização de sistemas de videovigilância em táxis
Lei 34/ 2013 – utilização de sistemas de videovigilância pelos serviços de segurança privada e de autoproteção

Tabela 12 - Legislação e Normas relativas à Videovigilância em Portugal

Da legislação/normas mencionadas anteriormente, apenas o Decreto-Lei 207/2005 é dedicado a regulamentar a prática de videovigilância por entidades públicas. Por lei, as forças de segurança pública (GNR, PSP e Polícia Pública) devem comunicar a existência e localização dos seus equipamentos de vigilância eletrónica à CNPD, que disponibiliza aos cidadãos essa informação de uma forma acessível e pública no seu *website*. No âmbito da presente lei, a utilização de videovigilância só autorizada nos seguintes casos:

- Proteção de edifícios e instalações públicos e respetivos acessos;
- Proteção de instalações com interesse para a defesa e a segurança;
- Proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência;
- Prevenção e repressão de infrações estradais;
- Prevenção de atos terroristas;
- Proteção florestal e deteção de incêndios florestais.[126]

[126] Complementar com a Lei 1/ 2005.

A CNPD prestou especial atenção a desafios da inovação tecnológica como identificação por radiofrequência; utilização de geolocalização; perfilagem automática e drones, mas implicitamente dirige-se principalmente a empresas do sector público e não à utilização destes dados pelo governo para controlo e prevenção.

No que diz respeito à transferência de dados pessoais para terceiros, esta é permitida livremente para outro estado membro da EU (mediante notificação à CNPD), e permitida condicionalmente para não-membros pois o RGPD consoante o nível de adequabilidade e capacidade de proteção de dados do país e possível compromisso contratual (RAUL, 2017). Recentemente, a Comissão Europeia adotou a *framework Privacy S*hield[127] que regulariza as transações de dados pessoais entre a UE e os EUA[128] para fins comerciais. Esta *framework* visa principalmente obrigar os EUA a proteger os dados fundamentais dos europeus.

Em Portugal, o código criminal prevê e autoriza a interceção de comunicações privadas em circunstâncias restritas e aprovadas pelo tribunal. Alusivo à conservação de dados das comunicações eletrónicas, a Lei 32/2008 requer o tratamento dos dados recolhidos em comunicações em rede de comunicações públicas. Esta atividade exige o registo da data, localização e identificação do utilizador do serviço, caso possível. O prazo de conservação é de 1 ano a partir da data de comunicação mas o acesso lícito a esses dados só é permitido consoante uma ordem judicial e para efeitos de investigação (RAUL, 2017).

[127] Em substituição do acordo *International Safe Harbor Privacy Princi*ples considerado obsoleto.

[128] Fonte: <http://europa.eu/rapid/press-release_IP-16-216_en.htm>.

d) Análise prática e comparativa das ciberestratégias

Existem diferentes abordagens para responder a esta nova classe de riscos, não só a nível organizacional e político, como económico e tecnológico, podendo a ciberestratégia ser representativa do investimento e preocupação de cada país sobre esta matéria.[129]

Os direitos e liberdades dos cidadãos são concedidos legislativamente pelas constituições de cada país e opcionalmente pela Declaração Universal dos Direitos Humanos. A DUDH distingue-se de outros documentos vinculativos por introduzir as questões de dignidade e, por isso, apontado como uma referência ética na conduta internacional. O apelo à subscrição deste acordo global foi feito visando a manutenção da paz e da segurança internacional e para, de certa forma, limitar as violações éticas que são previstas e autorizadas por lei para defesa nacional. A legislação, de forma direta ou indireta, esclarece que a vigilância deve ser discriminada, ou seja, os cidadãos têm que ser realmente suspeitos de serem uma ameaça para a segurança de um país.

Em matéria de segurança nacional, o governo é a autoridade absoluta e decisiva relativamente ao modo de operação de prevenção a uma ameaça ou reação a um ataque. Os regimes de governo dos três países são diferentes pelo que poderá ser um fator diferenciador na tomada de decisão.

O regime de governo dos EUA é presidencialista, ou seja, o poder executivo de administração dos interesses públicos é liderado pelo presidente mas a função legislativa e judiciária é exercida por órgãos dotados de autonomia para a execução das suas funções, ainda que de carácter público. Tal como a Rússia, os EUA são classificados como sendo uma federação visto serem compostos por estados com governo próprio. Não obstante, em última instância os estados estão sujeitos à regência da presidência. Os limites geográficos que dividem os estados federais russos – entre eles Moscovo, São Petersburgo e Sebastopol - não estão tão bem definidos como nos EUA mas estão estabelecidos detalhadamente no art.º 65 da Constituição. Ao contrário do regime norte-americano, Portugal e a Rússia são duas repúblicas semipresidencialistas, o que

[129] Cumprindo a metodologia comparativa, foi construída uma matriz de dados que sistematiza as principais características identificadoras dos três países (unidades de análise) segundo diferentes aspectos (níveis de análise). Essa matriz está disponível em Anexo.

significa que o poder executivo é partilhado entre presidente, primeiro-ministro e o conselho de ministros. Desta amostra, Portugal é o único estado unitário o que na prática significa que os organismo públicos pertencente ao Estado estão sujeitos ao comando do governo central[130]. Todos eles podem ser nomeados como uma república constitucional tendo em conta que a atuação do governo, incluindo a de todos os seus representantes, está de acordo com a lei constitucional que protege os cidadãos das possíveis atividades questionáveis do estado.

Verificou-se que todas as constituições preveem a prescrição dos direitos dos civis se autorizado por um órgão ou agência de poder jurídico ou legal e/ou se for evidente o risco para a segurança nacional. Ao longo dos últimos anos foram assinalas anulabilidades dos direitos de licitude questionável por parte do governo.

No mundo digital, a Quarta Emenda da Constituição dos Estados Unidos da América aplica-se à investigação e apreensão de dispositivos eletrónicos. Após os ataques terroristas de 11 de setembro de 2001 ao World Trade Center e ao Pentágono, a legislação foi promulgada para estender legalmente a permissão de recolha de informações, através do US Patiot Act[131]. Admitido como um esforço para erradicar conspirações terroristas, é do conhecimento público de que a NSA recolhe secretamente registos telefónicos, atividade que pode ser justificado pela interpretação das premissas acima mencionadas. À partida, as empresas de telecomunicações como a Verizon Business Network Services, não têm obrigação (nem devem) fornecer os registos dos seus clientes, exceto nas situações anteriormente previstas no capítulo VI, subcapítulo a). Porém, sob aprovação do Tribunal Secreto e através de um pedido[132] que ordenava a partilha dos dados dos seus clientes, a Verizon foi forçada legalmente a fornecer os dados telefónicos[133] de milhões de clientes americanos. Este documento revela que a recolha é total e a análise é feita independentemente de o indivíduo ser suspeito ou não

[130] Como anteriormente referido, as Regiões Autónomas dos Açores e Madeira são governadas por um representante nomeado pelo Presidente da República, ou seja, embora exisita uma ligação política, não existe dependência pois estas regiões tem autonomia absoluta na Proteção Civil Nacional.

[131] Fonte: <https://www.congress.gov/107/bills/hr3162/BILLS-107hr3162enr.pdf>.

[132] Disponibilizado pelo jornal The Guardian. Fonte: <https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>.

[133] Exclusivo aos metadados, ou seja, dados de localização, identificadores exclusivos e duração da chamada. O contéudo não é partilhado.

de qualquer delito[134], o que é contraditório à FISA. Para além de enfraquecer a relação entre os civis e o governo, este tipo de atividades aparentemente sem critério, tem um impacto abismal para credibilidade e confiabilidade dos clientes nas empresas. Para efeitos de segurança nacional, os organismos governamentais, os tribunais e partes envolvidas em litígios civis recorrem não só a empresas de telecomunicações como de serviços *online* como a Google. No Relatório de Transparência da Google[135], a empresa indica que:

"se um organismo fora dos EUA passar por um processo diplomático como o MLAT (Mutual Legal Assistance Treaty – Tratado de Assistência Jurídica Mútua) para obter uma intimação, ordem judicial ou mandado de busca da ECPA emitida nos EUA, a Google produzirá as mesmas informações que seriam produzidas se o pedido tivesse tido origem direta num organismo dos EUA. Nos casos em que a Google cumpra o processo judicial emitido diretamente pelo organismo fora dos EUA, as informações divulgadas podem incluir, por exemplo, informações de registo da Conta Google ou do YouTube (nome, informações de criação da conta e endereços de email associados), endereços IP de início de sessão recentes e carimbos de data e hora associados."

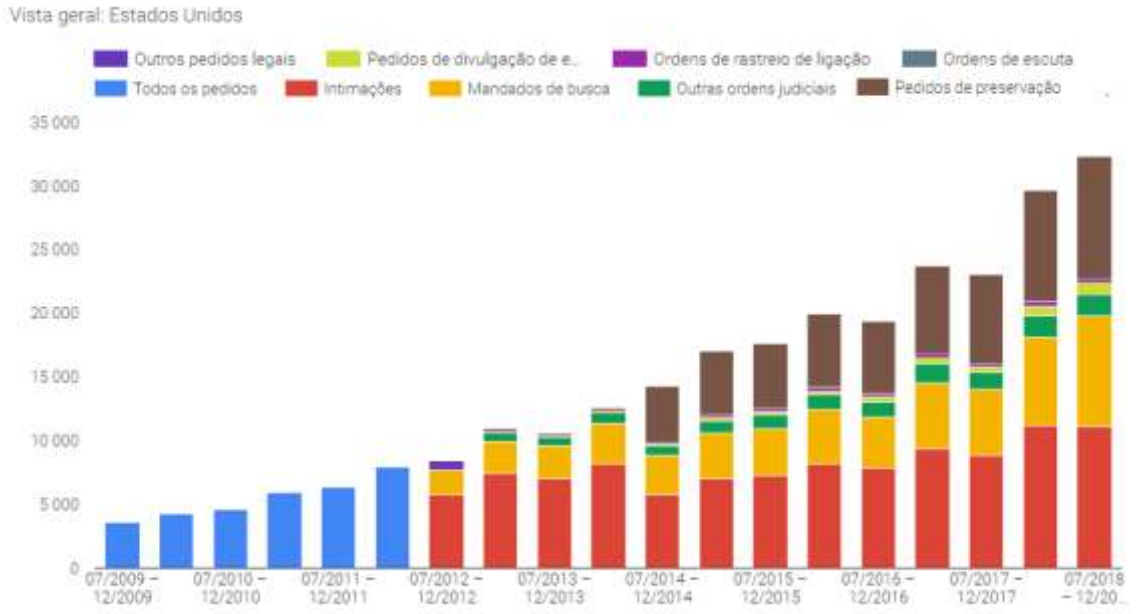

Figura 8 - Pedidos sobre utilizadores norte-americanos à Google

[134] Fonte: <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

[135] Fonte: <https://transparencyreport.google.com/user-data/overview?user_data_produced=authority:US;series:compliance&lu=user_data_produced>.

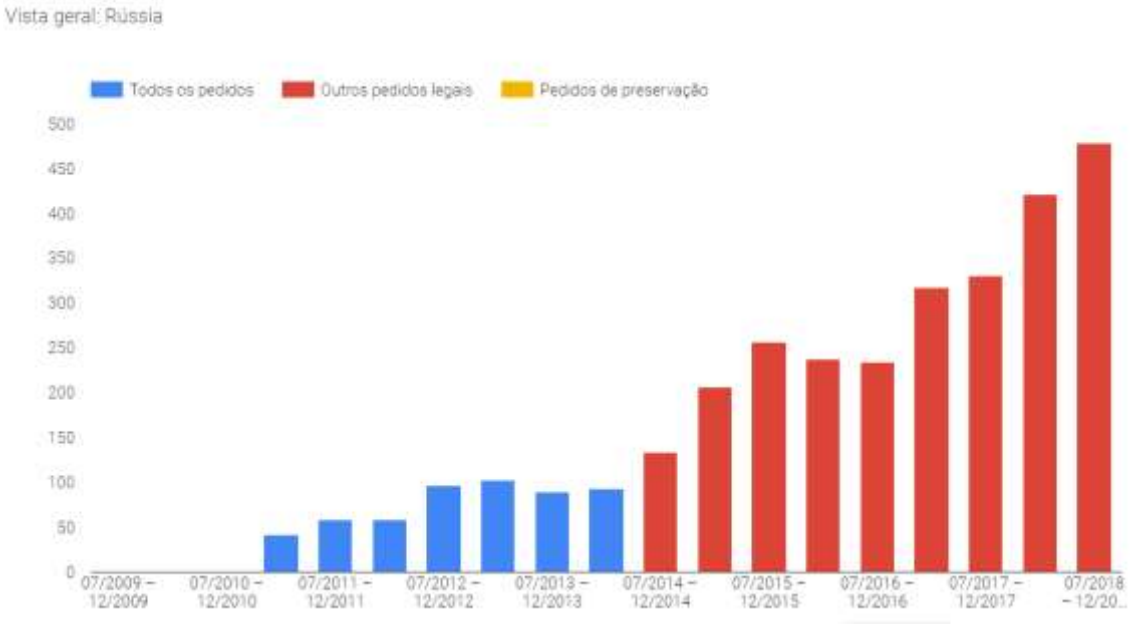

Figura 9 - Pedidos sobre utilizadores russos à Google

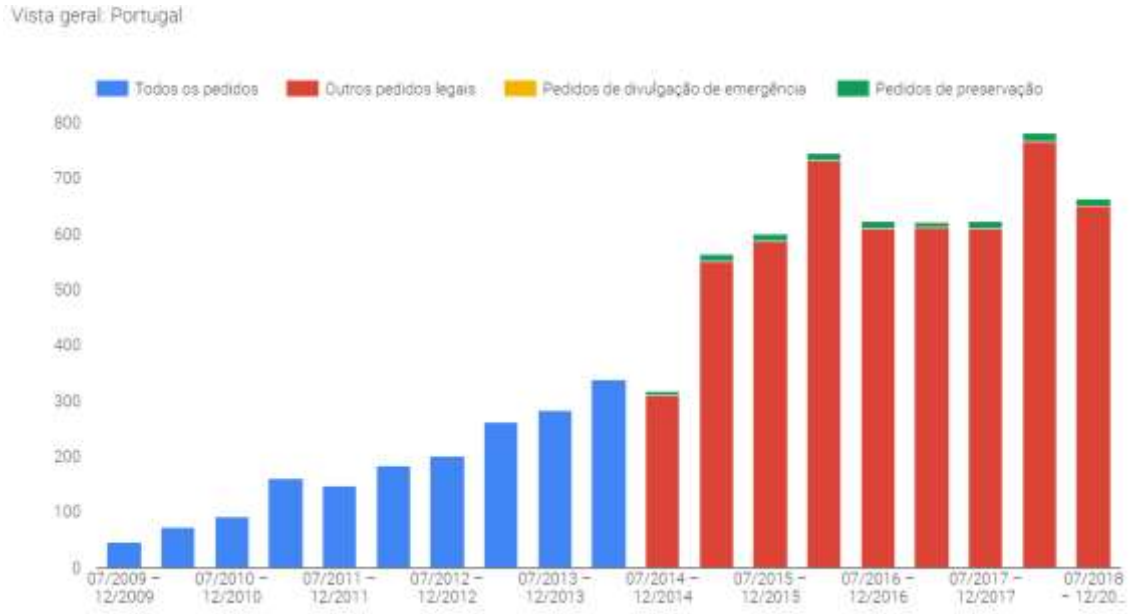

Figura 10 - Pedidos sobre utilizadores portugueses à Google

Pela análise dos gráficos, disponibilizados no relatório, é possível verificar que a empresa serviços online e *software* norte-americana recebeu sensivelmente 70 vezes mais pedidos dos EUA do que da Rússia durante o segundo semestre de 2018, e recebeu aproximadamente 50 vezes menos pedidos de Portugal do que dos Estados Unidos. A

tipologia dos pedidos é muito mais variada nos EUA[136], contemplado ordens de escuta e ordens de rastreio de ligação, que não são indicados para os outros dois países. À exceção de Portugal, em que o número de pedidos não é tão previsível, os pedidos dos Estados Unidos e da Rússia tendem a aumentar anualmente. A Google garante a validação dos requisitos legais aplicáveis e as políticas da Google em todos os pedidos e, se for considerado uma solicitação excessiva dadas as circunstâncias, a organização procura limitá-la pois a sua abordagem é sustentada pelo respeito pela privacidade e pela segurança dos dados armazenados dos seus clientes.

Em Portugal, a defesa do ciberespaço é fruto de uma sinergia entre o Estado e empresas privadas, visto que os sistemas e infraestruturas portugueses são operados pelo sector privado, bem como revelam inovação tecnologia e grande conhecimento. O mesmo tipo de relação não é observado nos outros dois países. O Departamento de Segurança dos Estados Unidos propôs uma "aliança" entre as empresas de tecnologia e o Governo, no entanto, algumas empresas privadas, como a Google e a Apple, decidiram apostar em medidas preventivas de codificação dos dados dos seus utilizadores e afastar-se da possibilidade de invasão de privacidade, de acordo com o Jornal Observador[137]. A manutenção do SORM[138], o sistema interno de vigilância russa direcionado a comunicações telefónicas e internet, é da responsabilidade do FSB (Connel & Vogler, 2017) e a sua introdução em 1995 exigia que as empresas de telecomunicações instalassem *hardware* do FSB para monitorizar as comunicações dos cidadãos russos. Estas "solicitações" aconteceram repetidamente durante os anos seguintes e foram estendidas a prestadores de serviços de internet e a ferramentas como redes sociais e e-mails (MARÉCHAL, 2017). Se, por um lado, o interesse pela desassociação das empresas privadas às operações estatais é cada vez mais frequentemente, por outro, a Apple parece alimentar a parceira com o governo ao possibilitar a ativação de alertas do governo do país do cliente no iPhone e no Apple

[136] Note-se que a leitura dos gráficos deve ser feita individualmente considerando que as legendas de cada gráfico são diferentes para cada um dos países.

[137] Fonte: <https://observador.pt/2015/04/21/eua-querem-alianca-com-empresas-de-tecnologia-em-nome-da-ciberseguranca/>.

[138] A sigla SORM corresponde ao seu nome em inglês System of Operational-Investigatory Measures

Watch [139]. Sensivelmente três meses após ter sido notificada pelo Ministério de Segurança Pública chinês que determinadas aplicações móveis – como o Skype ou WhatsApp - não estavam em concordância com as leis da China e por isso deviam ser retirados da AppStore[140], a empresa norte-americana escolhe uma empresa chinesa para contratar um serviço de armazenado. Para além da restrição do acesso à informação para clientes chineses, os dados dos clientes internacionais estavam disponíveis, ao abrigo da lei, se solicitados à empresa subcontratada para fins de investigação[141]. No início do ano, o Governo de Putin acusou o Facebook e o Twitter de violarem a lei de proteção de dados russa depois das redes sociais norte-americanas terem adotado uma nova lei de armazenamento de dados[142]. A preocupação com os dados dos seus cidadãos é de elogiar mas os interesses éticos por de trás desta intimidação pode não ser a evidente. Ainda que sejam participantes nas mesmas organizações, a relação EUA-Rússia é marcada por intensos conflitos e vão sempre agir suspeitando das intenções um do outro. Especulando sobre estes exemplos, o direito à informação é anulado pela ação de censura resultante da desconfiança pelo ex-inimigo.

Enquanto na Rússia e em Portugal o poder de decisão e influência se divide pelas duas figuras principais do governo (o Presidente e o Primeiro-Ministro), nos EUA a supremacia e as decisões são tomadas pelo Presidente americano, sejam eles legais, éticos ou não. Por outro lado, apesar de ser um regime semipresidencialista, pouco ou nada se ouve falar do Primeiro-Ministo russo Dmitri Medvedev ou de outros órgãos governamentais na resolução de conflitos internacionais. A autoridade de Putin parece ser soberana na Federação Russa e isso preocupa as outras nações e organismos defensoras dos direitos humanos. Não podemos considerar que Vladimir Putin tenha tido um percurso típico de ascensão política, como o de Donald Trump ou de Marcelo Rebelo de Sousa. O atual Presidente da Rússia, que tem estado envolvido no governo há precisamente vinte anos, foi agente da KGB e liderou os serviços secretos soviéticos FSB

[139] Fonte: <https://support.apple.com/pt-pt/HT202743>.

[140] Fonte: <https://observador.pt/2017/11/23/apple-retira-skype-da-sua-loja-de-aplicacoes-na-china-a-pedido-do-governo/>.

[141] Fonte: <https://www.dn.pt/mundo/interior/armazenamento-dos-dados-da-apple-na-china-gera-preocupacao-sobre-privacidade---ai-9149932.html>.

[142] Fonte: <https://pplware.sapo.pt/redes_sociais/russia-facebook-twitter-protecao-dados/>.

antes de se enveredar pela carreira política, o que certamente influenciou a sua postura e interpretação daquilo que é certo e errado em matéria de segurança nacional. Frequentemente culpabilizado de provocar instabilidade e conflitos internacionais, o comandante supremo das forças armadas russas afirmou na Conferência de Munique que "ninguém se sente a salvo […] porque ninguém consegue perceber que a lei internacional é como uma barreira que os protege".[143] Porém, se formos analisar a Constituição Russa, e do ponto vista prático, apenas o direito à privacidade de segredos pessoais e familiares não está sujeito a prescrição pelo estado (art.º 56), ou seja, a barreira que protege as pessoas singulares pode ser facilmente destruída se derrubada pelo governo nacional. A seção 29º do documento constitucional indica que "a todos é garantida a liberdade de pensamento e de expressão" e que "todos têm o direito de procurar, receber, transmitir, produzir e distribuir livremente informações de qualquer maneira legal [se não se tratar de um segredo federal", porém, no passado mês de Março, o parlamento aprovou a lei que autoriza as autoridades a multar quem desrespeite a sociedade russa e o governo no ciberespaço[144]. É certo que o parágrafo 2 indica a proibição de propaganda que incite o ódio nacional mas, o direito de liberdade à expressão é claramente posto em causa aqui, fazendo lembrar a censura do regime ditatorial português de Salazar. A credibilidade do estado é levada muito a sério pela Federação Russa e esta lei garante que sejam aplicadas medidas de uma forma legal mas também transparente. O que não é tão falado é como é que essas violações vão ser descobertas.

O uso da tecnologia para a melhoria da eficácia da atividade investigativa é cada vez mais intenso e frequente. As operações de inteligência são conduzidas eficientemente com o recurso a novos métodos de *data mining* que, embora autorizadas legalmente, são eticamente discutíveis. A divulgação do programa PRISM de interceção de canais doméstica pelo ex-militar e administrador de sistemas da NSA Edward Snowden foi talvez o evento mais polémico de duelo ético em matéria de privacidade entre divulgar as operações secretas do governo americano e informar os

[143] Tradução livre do discurso de Vladimir Putin acerca da discussão da política de segurança na Conferência de Munique em 2007. Fonte: <http://en.kremlin.ru/events/president/transcripts/24034>.

[144] Fonte: <https://ionline.sapo.pt/artigo/649164/r-ssia-proibe-desrespeito-ao-estado-e-supostas-fake-news?seccao=Mundo>.

cidadãos que estavam a ser vigiados constantemente. A recolha dos dados era feita envolvendo as bases de dados de empresas como a Google e o Facebook. Ao longo de meses, após a recolha de diversas provas das violações infringidas, Snowden serve-se dos media para difundir a sua descoberta. O ex-contratado da NSA foi formalmente acusado de espionagem e roubo de informação aos EUA e indiretamente ameaçado de morte por um funcionário do Pentágono.[145] Para a comunidade internacional, o norte-americano é considerado um herói por sacrificado a sua segurança pessoal em prol de um bem maior, tendo sido cogalardoado com o Sam Adams Award e o Ridenhour Priz.[146] Em parceria com a Fundação pela Liberdade de Imprensa, Snowden desenvolveu a Haven, uma aplicação *android* gratuita que utiliza os sensores de um *smartphone* para cruzar e produzir informação como o intuito de monitorizar e garantir que, principalmente profissionais de imprensa, possam exercer as suas atividades de uma forma segura e sem receio de estarem a ser vigiados[147].

Nos eventos pré-*cyber* de Pearl Harbor e Hiroshima foi possível observar que em tempo de guerra não houve preocupação relativamente à segurança dos civis, embora não fosse o alvo principal. Num confronto tradicional entre países, tudo o que é considerado como pertencente ou relacionado com o país adversário, é sinônimo de alvo a abater e os inimigos do alvo a bater podem ser potenciais aliados.[148] Se vigiar os "seus" é um ato preventivo e, por isso, interpretativamente justificável tendo em conta o clima de insegurança geral instalado, por outro, parece ser ainda mais aceitável espiar e controlar as ações dos outros[149] que possam comprometer a segurança nacional, estando ou não envolvido o domínio do ciberespaço. No passado mês de Junho, as forças iranianas advertiram os EUA de desrespeitarem a integridade territorial do Irão com o abate de um drone de vigilância militar. De acordo com o porta-voz da marinha, os EUA não fizeram nada para provocar este ataque contra um ativo de vigilância norte-

[145] Fonte: <https://oglobo.globo.com/mundo/advogado-de-snowden-pede-que-eua-respondam-sobre-ameacas-de-morte-contra-informante-11365418?topico=espionagem<

[146] O primeiro diz respeito à premiação de um profissional de serviços de inteligência que tenha agido com integridade e ética e o segundo reconhece os atos que protegem o interesse público, neste caso de exposição da verdade.

[147] Fonte: <https://guardianproject.github.io/haven/>.

[148] Não foi por coincidência que Snowden perdiu asilo a um dos grandes rivais dos EUA e a permissão da Rússia foi por acaso. Ambas as partes beneficiaram desta aliança.

[149] Entenda-se outros como outros governos, organismos e pessoas individuais de outras nacionalidades

americano que sobrevoava o espaço aéreo alegadamente internacional [150]. Em comunicações públicas, o comandante-chefe do IRGC[151] esclareceu que "o Irão não está à procura de guerra com nenhum país, mas [estão] totalmente preparados para defender o Irão"[152], sendo que este *mindset* é adotado por muitos países publicamente, como a Rússia e os Estados Unidos. Parece ser unânime que os governos pretendem evitar a transposição das tensões cibernéticas[153] para o campo de batalha físico, todavia, se necessário, não o evitarão. A defesa dos territórios - sejam eles físicos ou virtuais - é legítima e prevista pelo Manual de Tallin, no entanto, a problemática incide na escolha de uma postura hostil provocando instabilidade e imprevisibilidade nas relações internacionais. E Portugal, onde se situa e que postura adota?

Em Portugal o direito à privacidade bem como da proteção dos dados são assegurados pela legislação nacional e por diretrizes europeias. Ao contrário dos outros dois países, as ações de comprometimento da privacidade são supervisionadas não só por organismos português como órgãos extranacionais, como a Comissão Europeia. O RGPD, por ser documento como uma força jurídica dominante sob as leis particulares de cada estado-membro e não uma diretiva europeia, passou a ser diretamente aplicável em Portugal, todavia, foi evidenciada uma falta de adaptabilidade à lei nacional. Aquando da conclusão do prazo de tolerância para a implementação do RGPD, foi emitido um parecer (não vinculativo)[154] pela CNPD acerca da Proposta de Lei n.º 120/XIII/3.ª pelo Governo, que assegura a execução do RGPD na ordem jurídica nacional.

A autoridade de controlo portuguesa alertou para "várias indisposições" do Governo Português que "não respeitariam" e não estariam em conformidade com o novo regime de proteção de dados europeu. Entre outras incongruências, saliento a solução diferenciadora sugerida para o regime sancionatório de violações. Foi proposto

---

[150] É importante contextualizar este episódio: Em Maio de 2018, os EUA retiram-se unilateralmente do acordo entre o Irão e outras cinco potências, entre as quais a Rússia, ao reconhecer que o Irão excedeu o limite de reservas de urânio previsto pelo plano de ação. Fonte: <https://observador.pt/2019/07/01/russia-responsabiliza-eua-por-forcar-irao-a-quebrar-acordo-nuclear-e-apela-a-desdramatizacao/>.

[151] A sigla IRGC corresponde a *Islamic Revolutionary Guard Corps*.

[152] Fonte: <https://www.bbc.com/news/world-middle-east-48700965>.

[153] O conflito físico representa sempre perda económica e instabilidade nacional pelo que também não é benéfico para nenhuma das partes.

[154] Parecer N.º 20/2018. Fonte: <https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf>.

pelo Estado um regime excecional de isenção de coimas ao setor público nos próximos três anos, justificada pela previsão de que os "tratamentos realizados por entidades públicas […] podem prosseguir finalidades diferentes das que justificaram a recolha dos dados" [155], o que contraria a transparência, "viola ostensivamente o princípio da finalidade"[156] e quebra o direito à informação dos titulares. Ao longo dos últimos vinte anos, o regime sancionatório de violação de proteção de dados não foi diferenciado para os dois setores e esta discrepância entre o que é exigido ao público e ao privado provocaria certamente desigualdades na atribuição de responsabilidades e possivelmente descredibilização da importância proteção dos direitos dos cidadãos, baseada na tutela ou não do Estado. Após um ano de discussões e divergências, no passado mês de Junho, acabou por ser tomada uma decisão e aprovado um documento que prevê esta dispensa particular mas mediante aprovação pela CNPD.

A Estratégia Nacional para a Cibersegurança é só mais uma das provas do compromisso português com a segurança do ciberespaço e manutenção das relações internacionais de paz. Para além dos atos tradicionais de cibercrime, já são oficialmente identificadas ameaças com origem em agentes estatais por motivos políticos, militares ou económicos. Assim sendo, esta ciberestratégia confirma que é necessário desenvolver a disciplina da ciberdiplomacia. A abordagem da tradicional diplomacia internacional pode ser considerada como obsoleta pois exige métodos e estratégias hibridas para responder aos conflitos no ciberespaço, principalmente na aplicação do direito internacional (HEFFTER & GOEL, 1018).O conceito surgiu no início do milénio, como o aparecimento da internet e pela mão de autores visionários refletiam sobre o futuro das relações internacionais no mundo virtual, mas só agora é que tem ganho particular visibilidade como uma necessidade de implementação.

Se por um lado a União Europeia se preocupa tanto em conservar a privacidade das pessoas singulares e em definir leis uniformes de proteção dos dados, por outro, quer incutir uma lógica de autorregulação nos estados-membro, nomeadamente no

[155] Fonte: <https://www.publico.pt/2018/05/03/sociedade/noticia/comissao-de-protecao-de-dados-acusa-governo-de-desrespeitar-regulamento-europeu-1821661>.

[156] Fonte: <http://exameinformatica.sapo.pt/noticias/mercados/2018-05-03-CNPD-aponta-violacoes-e-copias-palavra-a-palavra-na-proposta-do-Governo-para-a-protecao-de-dados>.

âmbito da videovigilância. Estas limitações do emprego desta atividade[157] mantêm-se mas as organizações portuguesas do sector privado e público deixaram de obedecer à necessidade do controlo prévio da autoridade pública CNPD, estando sujeitos na mesma a fiscalização *a posteriori*. Isto representa um decréscimo enorme de pedidos à CNPD, o que é favorável ao seu funcionamento, mas obriga a que as empresas recorram a serviços de consultoria (mais caros) para a avaliação de impacto visto não deterem conhecimento sobre o tema.[158]

Desde a altura dos Descobrimentos, Portugal sempre foi conhecido por ocupar uma posição geográfica favorável, sendo a "porta de entrada" para a Europa. Ainda que nos tempos modernos o espaço físico já não seja tão importante como antigamente, pelo recurso ao ciberespaço, a reputação geográfica ainda importa. Devin Nunes, responsável pela coordenação política dos serviços de *intelligence* norte-americanos[159], tem sido um dos principais responsáveis em dialogar a aliança militar entre Portugal e os Estados Unidos, principalmente porque o país europeu poderia tornar-se num dos principais aliados na vigilância marítima do Oceânio Atlântico, na condicionante de um investimento na Marinha por Portugal. O congressista luso-descente ponderou a possibilidade de instalar um centro de processamento de informação da NSA na Base das Lajes, na Ilha Terceira (Açores), onde já existe uma base militar americana que teve um papel muito importante durante a Guerra Fria, contudo, esta hipótese foi considerada inválida pela NSA e pela CIA porque desconfiaram das capacidades das secretas portuguesas em lidar com os dados confidenciais norte-americanos[160].

Ao contrário dos dois outros países em análise, Portugal adota uma postura muito mais passiva e distante relativamente aos temas em que se foca esta dissertação mas isso não significa que Portugal esteja menos comprometido com a proteção do que os Estados Unidos ou a Rússia – talvez pelo contrário. Daquilo que foi possível apurar, não foi encontrado nenhum caso em que Portugal tenha estado diretamente envolvido

[157] São exemplos dessas limitações o prazo definido de conservação das imagens de 30 dias e a proibição de apontar as cameras para a a via pública.

[158] Fonte: <https://www.publico.pt/2018/04/30/sociedade/noticia/instalacao-de-videovigilancia-vai-deixar-de-ter-controlo-previo-1815738>.

[159] O que contempla a gestão das investigações do caso de Snowden e da possível interferência da Rússia na campanha eleitoral dos EUA em 2016

[160] Fonte: <https://www.publico.pt/2018/04/27/politica/noticia/centro-da-nsa-foi-falado-para-base-das-lajes-1815487>.

uma situação de ciberataque entre países, ou que tenha violado conscientemente os direitos dos portugueses, com a finalidade de proteger a nação, e isso também pode justificar o acompanhamento discreto e cordial dos conflitos pois está a acompanhar esta mudança de acontecimentos de uma forma teórica e não prática. Por pertencer à União Europeia, o seu comportamento iria ser possivelmente limitado mas nada garante que para fins de proteção nacional os direitos dos cidadãos não pudessem ser postos em segundo lugar. Acredito, contudo, que caso Portugal tivesse que tomar uma decisão deste calibre, o duelo ético interno possa ser maior.

De acordo com o Parlamento Europeu, a tensão UE-Rússia [161] tem-se intensificado nos últimos cinco anos por diversos episódios como o apoio da Rússia a grupos rebeldes no leste da Ucrânia, campanhas de desinformação e condutas internas questionáveis. Para a gestão da relação, a UE adota uma abordagem dupla: por um lado procura prevenir e resolver o conflito de uma forma diplomática, por outro ameaça aplicar sanções e cessar a cordialidade. Apesar de não estarem em concordância relativamente a algumas políticas, e por isso existir uma troca de acusações relativamente frequente, a relação transatlântica UE-EUA pode ser considerada mais sólida, amistosa, respeitadora, justificada possivelmente pela interdependência dos estados. Os três países têm a consciência que o conflito direto deve ser evitado e controlado, porque é benéfico para ambas as partes, mas assumem que serão sempre priorizados os seus ideias e formas de pensar.

O sucesso de muitas missões norte-americanas de inteligência assenta no sigilo de fontes, métodos e conteúdo e a adoção de políticas de transparência relativas à proteção de informações dos americanos pode parecer, à partida, sensivelmente antagónico e até antiético tendo em conta a missão da organização, contudo, é claramente evidenciado que a "transparência não significa que não [vão] manter as coisas apropriadamente secretas quando elas precisam ser mantidas em segredo", mas antes que é necessário "assegurar aos americanos que as suas informações [estão] adequadamente protegidas". Para além disso, algumas destas organizações promovem o direito à informação e à acessibilidade proporcionado, através do lançamento de documentos primários no website ou redes sociais, relacionados com as suas missões

[161] Fonte: <http://www.europarl.europa.eu/factsheets/en/sheet/177/russia>.

antigas[162]. Estes organismos querem (e precisam) que os cidadãos confiem neles para o exercício das suas funções mas as suas motivações, genuidade e praticidade pode ser questionável, podendo existir interesses de manipulação da sociedade para que esta se sinta estável e que, numa altura em que se desconfiança de tudo e de todos, o governo não seja um suspeito de detioração dos interesses civis. Quem por alguma razão puser em causa a confiabilidade e a credibilidade nacional será vítima de processos que podem tomar proporções gigantes, considerem-se os exemplos seguintes:

Snowden foi o grande divulgador dos programas de vigilância massiva nos Estados Unidos mas não foi o único partilhar documentos secretos norte-americanos. Julian Assange, jornalista autraliano, hacker e fundador do Wikileaks[163] – tornou de conhecimento público o envolvimento dos EUA na morte de civis iraquianos. Enquanto que Assange rege-se pelos princípios éticos do jornalismo como a utilidade pública, a objetividade e a verdade, Snowden (tal como a informadora do Wikileaks Chelsea Manning[164]) teve que pôr em causa a sua ética profissional, incorrendo em violações extremamente graves aos olhos do estado, em função do respeito pelos seus valores pessoais e moral. Tal como Assange, e embora não esteja diretamente relacionado com o governo, o português Rui Pinto considerou de interesse público a divulgação de documentos relacionados com práticas ilícitas no mundo do futebol. As motivações de Assange e Pinto não eram precisamente iguais visto que, Pinto tentou tirar benefício da posse de informação confidencial e extorquir dinheiro a troco da não divulgação. Atualmente, Rui Pinto está em prisão preventiva; a Assange foi cancelado o direito ao asilo; Após perdão concedido por Barack Obama em 2017, Manning voltou a ser detida por não testemunhar contra a Wikileaks; e a Rússia estendeu o asilo de Snowden até 2020. Estes atos são positivamente aceites pela comunidade civil e normalmente resultam em descredibilização das figuras que violam os direitos humanos.

[162] Fonte: <https://www.cia.gov/library/readingroom/collection/crest-25-year-program-archive>.

[163] Organização internacional sem fins lucrativos que tem como principal missão a análise e publicação de materiais oficiais censurados ou restritos que envolvem guerra, espionagem e corrupção. Esta organização já foi premiada por diferentes entidades de jornalismo e indicada para o nobel da paz por seis anos consecutivos. Fonte: <https://wikileaks.org/What-is-WikiLeaks.html>.

[164]Chelsea Manning é transsexual por isso pode ser reconhecida como Bradley Manning. Manning tem afiliação militar.

PRINCIPAIS IDEIAS

A guerra económica, tecnológica, política e ideológica pela conquista de zonas de influência é agora alargada ao quinto domínio de operações, o ciberespaço.

A legislação nacional dos países analisados prevê constitucionalmente limitações e proibições de invasão da privacidade das pessoas singulares mas, como comprovado pelos exemplos mencionados, essas imposições são contornáveis.

Os Presidentes são figuras políticas muito fortes e influentes, com um perfil dominante e habituados ao poder soberano. As duas superpotências têm um enorme historial de conflitos internacionais e, até aos dias de hoje, e embora publicitem uma relação cordial, disputam entre si o domínio económico, político, tecnológico e, agora, do ciberespaço. O desejo pela conquista, afirmação e hegemonia portuguesa é intrínseca à sua génese mas, presentemente, Portugal adota uma postura pacífica e apaziguadora nos conflitos internacionais e normalmente em conjunto com outras nações e organismos que foram alianças de estímulo da cooperação internacional. Embora seja reconhecida alguma capacidade tecnológica, Portugal não representa uma ameaça para as superpotências mundiais por diferentes razões: é um país pequeno de recursos limitados, o poder económico e de investimento no ciberespaço é pequeno quando comparado aos outros dois países e a parece adotar uma postura ética.

Em contexto de segurança nacional, os três países têm definidas as limitações para a invasão da privacidade dos cidadãos e cooperam com organizações internacionais como a NATO e a ONU. A grande diferença reside no controlo e supervisão das atividades governamentais. Enquanto que os EUA e a Rússia tem um vínculo voluntário baseado no compromisso, Portugal, para além disso, é subordinado economicamente e politicamente à União Europeia e às suas diretrizes. Isto não significa que a NATO, a ONU e a Amnistia Internacional não tenham poder de execução de medidas para impedir ou sancionar a violação dos direitos humanos, apenas a força, rapidez e eficácia pode não ser a mesma.

De acordo com o Manual de Tallin um Estado "afetado por um ato internacionalmente ilícito pode recorrer a contramedidas proporcionais, incluindo contramedidas cibernéticas, contra o Estado responsável" contudo o reconhecer o estado responsável é uma tarefa extremamente difícil. Por vezes é descoberto o

endereço *Internet Protocol*, ou abreviadamente IP, ou a rede onde se difundiu o ataque mas estes dados identificativos podem ser mascarado com o auxílio a ferramentas instaladas na máquina e por isso nunca foram encontradas provas suficientes para atribuição de um ciberataque a um estado. Relativamente ao uso da força, o Manual de Tallin reforça várias vezes a necessidade de proporcionalidade entre contra-ataques mas se um país tiver mais poder tecnológico, é previsível que use essa vantagem em seu benefício. É destacado que a população civil não deve ser objeto de ciberataque nem os seus pertences (incluindo computadores e redes de computadores) e é proibido privar deliberadamente os civis de nutrição (incluindo água) como método de ciberguerra mas espera-se que os ataques a infraestruturas aumentem, considerando que são uma forma de fragilizar o país inimigo.

Alegadamente justificada pela prevenção contra o terrorismo, observa-se que a vigilância massiva e indiscriminada é uma expressão de controlo social e (ab)uso da força governamental nos estados modernos e, normalmente, sob indicação e aprovação da figura máxima de autoridade. As diversas formas de recolha de informações, incluindo a ciberespionagem, direcionadas a um adversário durante um conflito armado não violam a lei do conflito armado, de acordo com o Manual de Tallin, mas esta permissão só é válida caso já existia uma ciberguerra e não de forma preventiva. Complementarmente, constata-se que os EUA e a Rússia, tidos em conta como governos liberais que promovem o direito à informação e a liberdade de expressão, conduziram operações de censura da opinião e restringiram de alguma forma o acesso à informação.

Observa-se uma lacuna na limitação do uso disciplinado da utilização de drones. O impacto da utilização na vida privada dos cidadãos é calculado mas a vulgarização desta tecnologia é relativamente recente, pelo menos de forma pública, pelo que ainda não está contemplada legislativamente.

De acordo com Passos (2017), o dilema de qualificar um ciberataque como ato de ciberguerra compreende não só questões de direito internacional adaptado à era da informação digital como também questões práticas como o impacto real no comprometimento nos direitos dos cidadãos. Existem realmente diretrizes internacionais neste âmbito mas o impacto real dificilmente é apresentado, bem como as sanções do comprometimento dos direitos humanos para a defesa nacional.

VII. CONSIDERAÇÕES FINAIS

A descoberta da internet originou numa alteração do *workflow* de informação e numa promoção da interconexão entre pessoas e países. Hoje em dia, o nosso dia-a-dia é marcado pela forte dependência e a confiabilidade na memória das máquinas, sejam eles computadores, servidores ou telemóveis, e caracterizado pela disponibilização voluntária cada vez mais intensa de dados pessoais de forma pública nas redes sociais. Este vínculo não existe só entre indivíduo-máquina mas também, numa escala ainda maior, entre organização/empresa/agência-máquina. A privação do uso desta extensão virtual causaria distúrbios sérios numa sociedade moderna principalmente porque, no caso dos indivíduos, raramente existe um *backup* da informação digital – falo em números de telefone, exames médicos, faturas digitais, etc. – sendo, hoje em dia, a nossa projeção no ciberespaço e pegada digital diária. Durante muitos anos, e não apenas para este contexto em específico, o benefício imediato tende a surgir e a ser mostrado primeiro, conquistando adeptos, mas a dúvida acerca da sua licitude tende a acontecer mais tarde. A discussão ética acerca do tratamento dos dados (frequentemente dados pessoais) que registamos na internet todos os dias tem ganho relevância nos últimos anos, contudo, é percetível que aconteceu bem mais tarde do que o fenómeno de registo, ou seja, durante muitos anos, e não só para a vantagem superou o fundamento de licitude. À medida que surgem novos desenvolvimentos tecnológicos, a importância da privacidade parece ser posta em segundo plano, até mesmo pela própria sociedade. Isto pode ser justificado pela falta de sensibilização ou porque os indivíduos não foram diretamente afetados por uma violação da sua privacidade.

A privacidade foi considerada um aspeto importante na vida em sociedade nos últimos séculos, mesmo antes do aparecimento da internet nas nossas vidas. A revolução tecnológica, a globalização, o fluxo transfronteiriço dos dados pessoais e conseguinte transformação digital originou novos desafios que facilitam às organizações do sector privado e público o uso de dados pessoais numa escala sem precedentes no exercício das suas atividades. A Carta dos Direitos Fundamentais da União Europeia, o RGPD, a EPCA, a FISA, entre outros, pretendem conferir algum tipo de coerência no

tratamento (incluindo recolha e armazenamento) dos dados de pessoas singulares. É importante destacar que, em diferentes fases da história internacional, os países em questão conduziram atividades de espionagem, muito antes do aparecimento da internet, a grande diferença é que a tecnologia, como o sistema de vigilância PRISM utilizado até 2013 nos EUA, facilitou e ampliou esta prática. Com isto não é pretendido que o tratamento dos dados seja interpretado como errado, muito pelo contrário pois o tratamento dos dados confere conhecimento, mas devem ser contempladas limitações legais, visto que as limitações éticas são facultativas.

É evidente que o mundo digital e a internet trouxeram-nos muitas oportunidades, principalmente a facilidade do direito do acesso à informação e a simplificação das comunicações internacionais mas, por outro lado, abriram um canal para o cibercrime e para a invasão da privacidade à distância por outros, nomeadamente pelo governo. É verifico um défice entre o número de casos de cibercrime (considerando aqueles identificados) e aqueles que realmente tiveram consequências para o criminoso, portanto, é expectável que as violações no ciberespaço por governo também não sejam todas descobertas ou sancionadas judicialmente pois as transgressões são dificilmente condenadas, principalmente se alegadas como segurança nacional.

De acordo com o SIED, "as informações são um instrumento essencial de apoio à decisão política, contribuindo para a segurança, salvaguarda e defesa dos interesses nacionais". Em prol de um suposto bem maior de segurança nacional, a privacidade de civis pode ser posta em segundo lugar em situação de vigilância controlo digital. As novas manobras de ataque requerem um maior conhecimento e inovação técnica bem como criatividade, mas, principalmente, exigem novas formas e estratégias de defesa. Embora o reforço da segurança das infraestruturas seja um objetivo legítimo e compreensível pela evidente importância que o caracteriza, as táticas utilizadas para justificar as ciberestratégias poderão ser contraproducentes no sentido em que, embora visem a segurança da sociedade num todo, têm um impacto negativo na segurança individual. As vulnerabilidades (físicas, lógicas e sociais) passaram a ser uma constante preocupação e, por isso, uma prioridade para os governos.

Compreender o comportamento de países com características tão distintas, num ambiente de ciberespaço, mostrou ser um verdadeiro desafio. À semelhança da Guerra Fria do século XX, a tensão e a disputa pela superioridade mundial contínua presente,

mas desta vez alargada a outras superpotências[165] como a China. Embora alguns neguem a hipótese de uma Segunda Guerra Fria, outros preveem que esta começará com uma violação da segurança europeia e do direito internacional por parte da Rússia e que isso causará que se formem duas forças competitivas: Rússia vs. Ocidente (nomeadamente Estados Unidos e a União Europeia), sendo que existe a possibilidade de outros países como a Síria, Afeganistão ou China de se aliarem à Rússia.

É frequentemente sugerido que os Estados Unidos da América apresentam uma lacuna relativa à legislação da privacidade. Ao longo desta investigação foi possível concluir que, na verdade, legislação existe e estão previstas restrições e proibições para o tratamento de dados pessoais dos cidadãos, contudo, verifica-se que algumas leis e normas de privacidade podem ser descartadas se aprovadas em tribunal. O Foreign Intelligence Surveillance Court dos Estados Unidos é um organismo federal e, por isso, dependente do governo e sob a sua jurisdição. Pressupõem-se que o poder e avaliação judicial seja efetuada de uma forma imparcial mas, tendo em conta todos os episódios de violação de privacidade divulgados e alguns deles autorizados, é impossível afirmar com certeza de que a aprovação é isenta, neutra e sem intromissão do governo norte-americano.

Para Portugal, o regime de proteção de dados e privacidade está previsto (não só mas principalmente) no novo Regulamento Geral de Proteção de Dados. Este direito europeu prevalece sobre as leis deste foro de cada país e o seu controlo é não só feito pela Comissão Europeia e pela entidade controlo nacional, no caso de Portugal a CNPD, como os outros estados membro estão atentos às possíveis violações. Ainda que organizações como a Amnistia Internacional ou a NATO supervisionem internacionalmente determinados assuntos relacionados com os direitos humanos, nomeadamente a privacidade e, em última instância, com a ciberguerra, os EUA e a Rússia são países independentes nesta matéria, sendo essa uma das diferenças entre os países analisados. Da investigação, averigua-se que a ciberguerra não foi declarada por nenhum país, contudo, os Estados Unidos e a Rússia já admitiram que estão preparados para se defenderem contra eventuais ataques, embora diplomaticamente o estejam a

[165] Superpotência é uma nação que se destaca pelo seu poder político, económico e militar. Fonte: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/superpot%C3%AAncia>

evitar. Ainda que não se tenha iniciado uma ciberguerra, a tensão está presente e já foram praticados ataques preparatórios.

Principalmente durante os mandatos do ex-presidente Barack Obama, foram observados esforços bipartidários para a execução do direito à privacidade: por um lado era evidente a necessidade de proteger os civis e os seus dados, por outro, a missão suprema do país é assegurar a proteção nacional, o que, à vista de alguns atores governamentais pode compensar por parecer que a proteção é para algo maior, e que até inclui os próprios civis. Muitas vezes a licitude dessa vigilância massiva é questionável tendo em conta que, na teoria e na sua generalidade, esta atividade é apenas autorizada se visar um determinado indivíduo e/ou em caso de perigo iminente. Enquanto que na União Europeia existem recursos efetivos para os cidadãos exporem situações de violação deste direito, por exemplo junto da CNPD, nos Estados Unidos e na Rússia não é tão claro como os afetados deverão proceder, para não mencionar que atividades executadas pelas agências secretas são dificilmente descobertas por um cidadão comum. Caso tenha sido o caso, é provável que o cidadão tenha descoberto a violação por aceder aos sistemas de informação dessas organizações e, legalmente, essa ação também é condenável.

Se já em 2013, o Pew Research Center chegou à conclusão de que 86% dos utilizadores[166] da internet já usaram formas de minimizar a visibilidade da sua pegada digital, recorrendo a diferentes estratégias - como apagar *cookies* e o histórico do browser; usar um nome falso e um endereço de email temporário; encriptar comunicações ou usar um serviço que permita navegar na internet de forma anónima – e, em determinados casos, evitar que os seus dados sejam acedidos por atores específicos – como hackers e criminosos, *advertisers*, governo e agências de autoridade – calcula-se que atualmente esse número não tenha diminuído.

De certa maneira, com a utilização da internet, aprendemos a aceitar com alguma normalidade esta realidade com o roubo de identidade, *hacking*, fraude de cartões de crédito mas é reconhecido que estes crimes podem ter cada vez consequências mais graves. O êxito defesa do ciberespaço e, a um nível mais alto, do

[166] A amostra deste inquérito nacional é de 1002 adultos (+18 anos). Inquérito *Anonymity, Privacy, and Security Online* disponível em: https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

país está sujeita diretamente ou indiretamente à atuação sinérgica dos organismos públicos (como ministérios, departamentos, tribunais, agências e forças militares), entidades privadas (de cibersegurança, de serviços online e relacionados com infraestruturas criticas), da comunidade académica e da própria sociedade civil. Para além das pessoas, a eficácia da segurança nacional é dependente da combinação de fatores como a tecnologia e políticas, particulares a cada país, bem como os valores éticos da recolha e uso da informação. As mudanças globais das realidades no mundo digital exigiram uma reordenação da agenda e ciberestratégias de segurança nacional, nomeadamente em adaptar a abordagem de recolha e tratamento de informações de pessoas singulares.

Ao longo desta investigação, foram identificadas as seguintes características relacionadas com a ciberguerra, segurança nacional é ética da informação:

- A dependência económica nos sistemas de informação é cada vez maior
- O setor privado de infraestruturas críticas é normalmente o alvo principal por ser mais fácil de atingir
- Os incidentes de segurança da informação são cada vez amplamente difundidos e estendidos a pessoas singulares
- Constantemente surgem novas formas de ataque e estratégias bem como novos tipos de armas
- Têm-se vindo a observar um aumento da procura de *hackers* para fortalecer as redes de computadores tanto para o setor público ou privado
- Em Portugal e na União Europeia observa-se um esforço para proteger os dados e a privacidade dos dados de uma forma preventiva e com uma tendência ética mas nos EUA e Rússia não é possível confirmar

Se reconhecermos que a evolução dos Sistemas de Informação é inevitável, é necessário ponderar riscos e construir sistemas mais resistentes. Sendo que a robustez dos sistemas por vezes é comprometida por desenvolvimentos em versões pouco testadas para dar resposta rápida a um problema, há que definir planos de contingência no que toca a boas práticas que diminuam a exposição dessas infraestruturas a possíveis ataques. Para além disso, no desenvolvimento de *softwares*, o princípio da privacidade por conceção e por defeito (*privacy by design* and *by default*) deve ser adotado.

A segurança nacional mostrou ser um tema interessante para a discussão do impacto das tecnologias de informação legislativo e ético nos direitos individuais, todavia, futuros estudos poderão contemplar a investigação de outros temas adjacentes ao foco desta dissertação. Muitas vezes, os *hackers* éticos não têm qualquer afiliação a esses organismos, e poderá ser interesse averiguar e entender os seus dilemas éticos respetivamente às "armas" e modelos de ação usados na ciberguerra. Para isso, era importante ter em conta a existência de serviço militar obrigatório, como acontece na Federação Russa.

Outra tendência que merece ser explorada prende-se com o uso da inteligência artificial (IA) como recurso de combate no ciberespaço[167]. Este é um modelo que poderá trazer inúmeros desafios éticos, principalmente numa altura em existe uma preferência por sistemas automáticos de resposta. Inclusive, em entrevista ao jornal Diário de Notícias, o investigador francês Charles Thibout, especialista em questões geopolíticas e estratégicas de tecnologias emergentes, afirma que a UE e os EUA têm um relacionamento diferente com a IA. Enquanto que nos Estados Unidos, "a tecnologia é vista como instrumento de emancipação dos homens", na União Europeia existe um certo receio da Inteligência Artificial, em parte pela influência negativa da indústria cinematográfica. Thibout acrescenta que a corrida é liderada pela China que, por aspirarem à posição de principal potência tecnológica do mundo, investem cerca de sete vez mais em IA do que os EUA. Apesar dos esforços da União Europeia, principalmente da França, em desenvolver esta tecnologia, a UE não está numa posição favorável de "competição", principalmente porque quando surge um produto inovador, existe uma grande probabilidade que este seja comprado pela China ou Estados Unidos.[168] Em paralelo, e segundo a plataforma Modern Diplomacy, também a Rússia reconhece a importância da Inteligência Artificial em cenário de ciberguerra, tendo até Vladimir Putin comentado que quem liderar esta nova tecnologia, irá governar o mundo.[169]

[167] Fonte: <https://futuretodayinstitute.com/2018-tech-trends-annual-report/>.

[168] Fonte: <https://www.dn.pt/mundo/interior/a-china-conta-com-a-inteligencia-artificial-para-se-tornar-a--primeira-potencia-mundial-9395620.html>.

[169] Fonte: <https://moderndiplomacy.eu/2018/04/19/the-artificial-intelligence-race-u-s-china-and-russia/>.

A reflexão sobre as ciberestratégias de segurança interna num mundo cada vez mais digital e a apresentação dos sistemas de proteção nacional particulares aos Estados Unidos, Rússia e Portugal nesta dissertação garantem o cumprimento de dois dos objetivos propostos para esta investigação.

Adicionalmente, também dentro do âmbito desta dissertação, pretendia-se investigar de que forma a segurança nacional pode comprometer os direitos humanos e se a ciberética pode efetivamente moderar as ciberoperações estatais. Este objetivo foi parcialmente cumprido. Ainda que com intensidades, formas e meios diferentes, os três estados mostram-se preocupados com os direitos humanos, neste caso com a privacidade e a liberdade de expressão das pessoas singulares. Foram identificados mecanismos que permitem aos governos contornar as restrições das leis de privacidade, como a justificação de uma ação de prevenção de terrorismo ou se obtida uma aprovação específica do tribunal responsável pelas validações dos pedidos[170], contudo, não foi encontrado nenhum documento normativo nacional que defina os limites éticos no tratamento da informação civil. Por essa razão não foi possível concluir nada de concreto relativamente à aplicação prática da ciberética em conflitos virtuais que envolvam os países em estudo. É possível especular sobre o assunto e dizer que dos três países, Portugal seria provavelmente o que agiria mais eticamente na iminência de uma ciberguerra, talvez por estar sob a alçada de organização maior com uma regulamentação extremamente sólida. Qualquer um dos estados, se apoiado pela NATO ou ONU[171], à partida as suas ciberestratégias e ciberoperações estariam aprovadas, legitimadas e controladas eticamente mas atualmente não se verificou nenhum caso prático desta situação. A invasão da privacidade em prol da segurança interna aparenta estar prevista numa espécie de "contrato social", fruto de um consentimento obrigatório dos civis.

Hoje, passado um ano desde que iniciei esta investigação, ainda não é consensual a concretização da ciberguerra: *já começou, está para acontecer* ou é só *uma especulação sobre o futuro que pode nem vir a tomar tamanhas proporções*? Alguns autores defendem o ciberataque à Estónia como o primeiro ato de ciberguerra de

[170] Esses tribuinais são públicos, ou seja, em última instância respondem ao Presidente.

[171] Ou se pelo menos se estiver de acordo com o *jus ad bellum*.

sempre; outros consideram a ciberguerra como uma possível realidade a curto-médio prazo e alguns creem que esta seja uma discussão hipotética, pelo menos para já. Estas diferentes perspetivas fizeram-me questionar acerca do âmbito desta dissertação – como é que eu iria conseguir investigar e refletir sobre algo que na realidade nem tinha ainda acontecido ou se tinha não era nos moldes previstos - mas, acima de tudo, propiciaram uma introspeção e aguçaram o meu sentido crítico de forma a definir qual era o meu entendimento sobre o assunto. A intensidade da tensão/conflito entre Rússia-USA, por exemplo, é visivelmente notória mas a forma como os estados interagem secretamente e as ciberoperações que executam para afetar o outro são muito menos divulgadas. Para mim, os ciberataques à Estónia, Geórgia ou EUA não foram atos de ciberguerra porque não envolveram contra-ataque mas foram atos preparatórios e exemplificativos do que pode acontecer no futuro se não controladas, reguladas e legisladas as ciberoperações.

VIII. REFERÊNCIAS BIBLIOGRÁFICAS

ALTMANN, J., & VIDAL, F. (2013). *Cyber Warfare.* Alemanha: International Review of Information Ethics. Obtido de http://www.i-r-i-e.net/inhalt/020/020-full.pdf

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. (2005). Glossário da Sociedade da Informação. Obtido de http://purl.pt/426/1/

AUSTIN, G., & MURAVIEV, A. (2000). *The Armed Forces of Russia in Asia.* New York, Estados Unidos: I.B. Tauris.

BANKS, W. C. (2016). *Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage* (Vol. 66). Georgia, Estados Unidos: Emory Law Journal. Obtido de http://law.emory.edu/elj/_documents/volumes/66/3/banks.pdf

BERTOLI, G., & MARVEL, L. (2017). Cyberspace Operations Collateral Damage - Reality or Misconception? *The Cyber Defense Review, 2*. Estados Unidos: Army Cyber Institute. Obtido de https://www.jstor.org/stable/26267385

CALCUTT, D. (1990). *Report of the Committee on Privacy and Related Matters.*

CALOYANNIDES, M. (2003). Privacy vs. Information Technology. *IEE Security & Privacy*, 100-103.

CAPURRO, R., ELDRED, M., & NAGEL, D. (2013). *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld.* Heusenstamm, Alemanha: Ontos Verlag. Obtido de https://www.arte-fact.org/dgtlwhns.pdf

CATH, C., GLORIOSO, L., & TADDEO, M. (2016). *NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' – A Report.* Springer.

CLAPPER, J. R., ROGERS, A. M., COMMANDER U. S. N., & COMMANDER U. C. (2017). Foreign cyber threats to the United States. Hampton Roads International Security Quarterly. Obtido de https://www.courthousenews.com/wp-content/uploads/2017/01/Joint-Statement.pdf

CLARKE, R., & KNAKE, R. (2014). The Next Threat to National Security and What to Do About It. Obtido de http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf

CNCS. (s.d.). Estratégias Nacionais de Cibersegurança . Obtido de https://academiamilitar.pt/images//Apresentacoes/1.Estrat-Seg-Ciberespao_CNCS.pdf

CONNELL, M., & VOGLER, S. (2017). Russia's Approach to Cyber Warfare. Virginia, Estados Unidos: Center for Naval Analyses. Obtido de https://apps.dtic.mil/dtic/tr/fulltext/u2/1032208.pdf

DEIBERT, R., ROHOZINSKI, R., & CRETE-NIISHIHATA, M. (2012). C*yclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war.* Security Dialogue.

DELAC, G., SILIC, M., & KROLO, J. (2011). *Emerging Security Threats for Mobile Platforms.* IEE.

DENNING, D. E. (1998). *Information Warfare and Security.* Estados Unidos: Addison-Wesley. Obtido de http://nnt.es/Information%20warfare%20and%20security.pdf

DIPERT, R. (2010). *The ethics of Cyberwarfare.* Journal of Military Ethics.

DUPONT, B. (2013). *The Proliferation of Cyber Security Strategies and their Implications for Privacy.* Circulation International de L'Information et Sécurité.

FARWELL, J., & ROHOZINSKI, R. (2011). *Stuxnet and the Future of Cyber War.* Londres, Inglaterra: Survival.

FLORIDI. (1999). Information Ethics: on the Philosophical Foundation of Computer Ethics.

FLORIDI, L. (2001). Information Ethics: An Environmental Approach to Digital Divide. Oxford, Inglaterra: Spring. Obtido de http://uhra.herts.ac.uk/bitstream/handle/2299/1833/902041.pdf?sequence=1

FLORIDINI, L. (1999). *Ethics and Information Technology.* Kluwer Academic Publishers. Obtido de https://doi.org/10.1023/A:1010018611096

GADY, F., & AUSTIN, G. (2010). *Russia, the United States and Cyber Diplomacy.* New York, Estados Unidos: EastWestInstitute. Obtido de https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

GOMES, E., & DA CRUZ, J. (2016). Estudo Comparado como Método de Pesquisa: os Ritos de Iniciação nas Religões Monoteístas. Recife, Brasil: Paralellus. Obtido de http://www.unicap.br/ojs/index.php/paralellus/article/view/645

GONÇALVES, J. (2016). *Enquadramento Legal da Cibersegurança em Portugal e no Mundo (Tese de Doutoramento).*

GREMBERGEN, W. V. (2004). Strategies for Information Technology Governance. Estados Unidos: Idea Group Publisher.

HALPIN, E., TREVORROW, P., WEBB, D., & WRIGHT, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs.* New York, Estados Unidos: Palgrave Macmillan.

HANTRAIS, L. (2009). International Comparative Research: Theory, Methods and Practice. Estados Unidos: Palgrave Macmillan.

HARDACH, G. (1981). *The First World War, 1914-1918.* California, Estados Unidos: University of California Press.

HEFFTER, A., & GOEL, S. (1018). *Mitigating Cyber Warfare through Deterrence and Diplomacy.* Obtido de https://www.albany.edu/wisp/papers/WISP2018_paper_18.pdf

HUGHES, D., & COLARIK, A. (2017). The Hierarchy of Cyber War Definitions. Springer.

INKSTER, N. (2016). Information warfare and the US presidential election.

INSTITUTO DA DEFESA NACIONAL. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa* (Vol. 28). Portugal: IDN Cadernos. Obtido de https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

KALDOR, M. (2007). *New and old wars: Organised violence in a global era.* California, Estados Unidos: Stanford University Press. Obtido de http://www.guillaumenicaise.com/wp-content/uploads/2014/08/Kaldor-New-Wars-.pdf

KIZZA, J. M. (2001). *Computer Network Security and Cyber Ethics.* Carolina do Norte, Estados Unidos: McFarland.

KIZZA, J. M. (2007). *Ethical and Social Issues in the Information Age.* Springer. Obtido de https://s3.amazonaws.com/academia.edu.documents/44184389/Ethical_and_Social_Issues_in_the_Information_Age-Springer_London_2013__5th_Joseph_Migga_Kizza.pdf?response-content-disposition=inline%3B%20filename%3DEthical_and_Social_Issues_in_the_Informa.pdf&X-A

KOLLOCK, P., & SMITH, M. (1999). *Communities in Cyberspace.* Londres, Inglaterra: Routledge.

KSHETRI, N. (2016). Cyberwar: China and the United Stated. Em *Handbook of US-China Relations.* Edward Elgar Publishing.

LATIMER, M. H. (2018). *Choosing Security Over Freedom: the Intersection of Technology and Privacy in a Post-9/11 World.* Arizona, Estados Unidos: University of Arizona. Obtido de https://repository.arizona.edu/bitstream/handle/10150/630350/azu_etd_hr_2018_0103_sip1_m.pdf?sequence=1&isAllowed=y

LAWSON, S., & MIDDLETON, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security in the United States, 1991-2016.

LEAVITT, N. (2005). *Mobile Phones: the Next Frontier for Hackers?*

LESSIG, L. (1999). *Code and Other Values for Cyberspace.* Basic Books.

LEVY, P. (1997). *Cyberculture. Éditions Odile Jacob.*

LEVY, S. (1984). *Hackers: Heroes of the Computer Revolution.* Anchor Press/Doubleday.

LIÑAN, A. P. (2007). *El Métdo Comparativo: Fundamentos y Desarollos Recients.* Pensilvânia, Estados Unidos: Universidade de Pittsburgh.

LOR, P. (2011). *International and Comparative Librarianship.*

MARÉCHAL, N. (2017). *Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet policy.* Cogitatio. Obtido de https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808

MORAG, N. (2018). *Comparative homeland Security: Global lessons*. John Wiley & Sons, 2018.

MORGAN, A. E. (2019). Government Surveillance and The War On Terror: Why is Government Cyber Data Collection Increasingly Sanctioned by the Courts, Despite The Development of Privacy Law Protections Against Domestic Surveillance Beginning in the Early Twentieth Century? Nova Jersey, Estados Unidos: Seton Hall University. Law School Student Scolarship. Obtido de https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1952&context=student_scholarship

NUNES, P. V. (2016). *Sociedade em Rede, Ciberespaço e Guerra de Informação.* Lisboa, Portugal: Instituto da Defesa Nacional.

PADEN, W. E. (2011). *Interpretar o sagrado: modos de conceber a religião.* Paulinas.

PALMER, W. (2001). *Engagement with the Past: the lives and works of the World War II.* Kentucky. Estados Unidos: University Press of Kentucky.

PASSOS, C. (2017). *Ciberguerra e Ciberpaz nas novas Relações Internacionais.* http://comum.rcaap.pt/bitstream/10400.26/21478/1/60_CapCarlosPassos_TII_VF.pdf. Pedrouços, Portugal: Instituto Universitário Militar.

RAMOS, H. (2013). *The Omniscient Digital Eye: The Role of Software Surveillance in Cyberwar's Power Dynamics.* Lisboa, Portugal: ISCTE – Instituto Universitário de Lisboa.

RAUL, A. C. (2017). *The Privacy, Data Protection and Cybersecurity Law Review.* Londres, Inglaterra: Law Business Research Limited. Obtido de https://thelawreviews.co.uk/digital_assets/b5f160ac-fb67-48da-be84-a085ee98b2f2/The-Privacy-Data-Protection-and-Cybersecurity-Edition-5.pdf

RAYMOND, E. (1996). *The New Hacker's Dictionary.* Boston, Estados Unidos: MIT Press.

REYNOLDS, G. (2011). *Ethics in Information Technology.* Nelson Education.

RICH, K. L. (2013). *Introduction to Ethics.* Obtido de http://samples.jbpub.com/9781449649005/22183_CH01_Pass3.pdf

ROWE, N. C. (2007). Ethics of Cyber War Attacks. Em L. JANCZEWSKI, & A. COLARIK, *Cyber Warfare and Cyber Terrorism.* Pensilvânia, Estados Unidos: Information Science Reference. Obtido de http://seo-accessibility.com/dbms/cyber-warfare-and-cyber-terrorism-premier-reference.9781591409915.31444.pdf#page=138

ROWE, N. C. (2010). *The Ethics of Cyberweapons in Warfare.* Ottawa, Canada: International Journal of Technoethics.

RUHMANN, I. (2013). *Cyber War: Will it Define the Limits to IT Security?* International Review of Information Ethics.

SAKWA, R. (2008). *Russian Politics and Society.* Routledge. Londres, Inglaterra: Obtido de http://www.untag-smd.ac.id/files/Perpustakaan_Digital_2/POLITICS%20AND%20GOVERNMENT%20Russian%20Politics%20and%20Society-.pdf

SANTOS. (2017). *Contributos para uma estratégia nacional de ciberdefesa.* Pedrouços, Portugal: Instituto Militar Universitário. Obtido de https://comum.rcaap.pt/bitstream/10400.26/24554/1/TII%20-%20COR%20TM%20Duarte%20Santos.pdf

SANTOS, P., BESSA, R., & PIMENTEL, C. (2008). *CyberWar - O Fenómeno, as Tecnologias e os Atores.* Lisboa, Portugal: FCA - Editora de Informática, Lda.

SCHMITT, M. N. (2013). *Tallin Manual on the International Law applicable to Cyber Warfare.* Cambridge, Reino Unido: Cambrigde University Press. Obtido de http://csef.ru/media/articles/3990/3990.pdf

SHAKARIAN, P. (2011). *The Russian Cyber Campaign Againsnt Georgia.* Military Review.

SIBONI, G., & SIMAN-TOV, D. (2014). *Cyberspace Extortion: North Korea versus the United States.* Tel Aviv, Israel: INSS Insight.

SILVA, N. (2015). A Ética do Militar no Século XXI. Em *IDN Brief.* Lisboa, Portugal: Instituto da Defesa Nacional. Obtido de https://comum.rcaap.pt/bitstream/10400.26/7829/1/idnbrief_janeiro2015.pdf

SIMÕES, I. d. (2009). *A Sociedade em Rede e a Cibercultura: Dialogando com o pensamento de Manuel Castells e de Pierre Lévy na era das novas Tecnologias de Comunicação.* Revista Eletrónica Temática. Obtido de http://canal.unigranrio.com.br/enade/publicidade-e-propaganda/downloads/tecnologia-em-comunicacao/artigo-sociedade-em-rede-ciberespaco-simoes.pdf

SPINELLO, R. (2010). *Cyberethics: Morality and Law in Cyberspace.* Massachusetts, Estados Unidos: Jones & Bartlett Learning.

TZU, S. (2006). *A Arte da Guerra.* Edições Sílabo (ed. Portuguesa).

U.S. DEPARTMENT OF DEFENSE. (2013). *Field Manual 1-02, Operational Terms and Graphics.* Estados Unidos: U.S. Department of Defense.

VALERIANO, B., JENSEN, B., & MANESS, R. (2008). *Cyber Strategy: The Evolving Character of Power and Coercion.* Oxford, Inglaterra: Oxford University Press.

WALL, D. S. (2005). *The Internet as a Conduit for Criminal Activity.* California, Estados Unidos: Thousand Oaks.

WARREN, S., & BRANDEIS, L. (1890). *The Right to Privacy.* Massachusetts, Estados Unidos: Harvard Law Review.

WEATHERSBY, K. (1993). *Soviet aims in Korea and the origins of the Korean War, 1945-1950: new evidence from Russian archives.* Florida, Estados Unidos: Florida State University. Obtido de http://pages.ucsd.edu/~bslantchev/courses/nss/documents/weathersby-soviet-aims-in-korea.pdf

WILKINSON, P. (2010). *International Relations.* New York, Estados Unidos: Sterling Publishing Company, Inc.

WILSON, C., & DRUMHILLER, N. (2016). US-China Relations: Cyberespionage and Cultural Bias. Em *National Security and Counterintelligence in the Era of Cyber Espionage.*

ZIMAN, K. (2018). *Privacy in Plain Sight: Fourth Amendment Considerations for the Collection, Retention, and Use of Data.* Estados Unidos: Homeland Security Affairs.

IX. ANEXO

	ESTADOS UNIDOS	RÚSSIA	PORTUGAL
CONTEXTO HISTÓRICO E GEOGRÁFICO	- Conjunto de estados com legislação própria mas dependentes do governo nacional - Participou nas duas guerras mundiais, embora tenha adotado inicialmente uma postura neutra - Superpotência com investimento tecnológico e postura competitiva - Foi vítima de grande ataque terrorista em 2001 por um grupo de Al-Qaeda	- País estabelecido geograficamente e politicamente há pouco tempo - Perdeu poder com a dissolução da URSS - Participou na primeira guerra mundial - Superpotência com investimento tecnológico e postura competitiva - Foi sugestionada a atribuição da autoria de alguns ciberataques internacionais a este país	- País consideravelmente menor geograficamente mas que esteve envolvido em inúmeros conflitos durante a era dos descobrimentos - País completamente autónomo mas é membro da aliança da UE e por isso rege-se em conformidade com as diretrizes europeias. - Participou na primeira guerra mundial - Investe em tecnologia mas menos do que os outros dois países
CONTEXTO POLÍTICO	- Federação presidencialista	- Federação semipresidencialista	- Unitário semipresidencialista
ORGANIZAÇÕES DE DEFESA NACIONAL E CIBERSEGURANÇA	- Agências atuam preventivamente, ativamente e reactivamente - As operações de inteligência e defesa são maioritariamente responsabilidade da NSA e CIA.	- Não foi encontrada informação suficiente para avaliar a postura de atuação - As operações de inteligência estão maioritariamente focadas no KGB	- Aparentam uma postura preventiva na sua maioria - Promovem boas práticas e a discussão da regulação do ciberespaço, ciberdiplomacia e cibercrime - Embora exista o GNS e o CNCS, a responsabilidade é distribuída por várias organizações
LEI DO CIBERCRIME	- O cibercrime é regulado *Network Crime Statutest*	- Não foi encontrada informação suficiente que garanta a existência de um regulamento ou lei específica neste âmbito	- O cibercrime está previsto legislativamente através da Lei do Cibercrime, tal como na UE
LEGISLAÇÃO E NORMAS DE PROTEÇÃO DE DADOS E PRIVACIDADE	- Direito à privacidade incluído na Constituição nacional e previstas exceções	- Direito à privacidade incluído na Constituição nacional e previstas exceções - Leis da Privacidade e Proteção de Dados muito focadas para o setor das telecomunicações e media e para sector privado principalmente - Não existe controlo externo destas leis	- Direito à privacidade incluído na Constituição nacional e previstas exceções mas sempre em conformidade com as diretrizes europeias - Controlo da aplicação das leis por uma autoridade externa (UE)

POSIÇÃO NO CONFLITO INTERNACIONAL	- Constante conflito e tensão com a Rússia, Coreia do Norte e China - Pretende evidenciar o seu poder no ciberespaço e, se necessário, dominar este novo universo	- Constante conflito e tensão principalmente com os EUA - A Rússia conferiu asilo a Snowden, acusado de roubo de informação norte-americana - Pretende evidenciar o seu poder no ciberespaço e, se necessário, dominar este novo universo	- Não tem conflito direto com nenhum país em concreto, embora, através da UE, tenha exprimido sua opinião relativamente ao modo de atuação de países como
RELAÇÃO COM ENTIDADES PRIVADAS	- Governo procura estabelecer alianças com as entidades privadas mas algumas não pretendem estar associadas ao governo porque poderá levar a uma descredibilização do negócio perante os seus clientes. - As empresas privadas são obrigadas a fornecer os dados dos clientes se essa solicitação for aprovada pelo Tribunal Secreto	- O governo russo tem como política o armazenamento dos dados em território nacional, por isso, as empresas em tenham servidores fora do território, estão sujeitos ao bloqueio - Não é evidente à partida uma colaboração sólida	- Parceria colaborativa com benefício para ambas as partes

Tabela 13 - Matriz de comparação de ciberestratégias dos EUA, Rússia e Portugal