CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

POLÍTICAS PÚBLICAS

NOVEMBRO DE 2021

FICHA TÉCNICA

AUTORIA DO ESTUDO

Rui Pedro Lourenço (Coord.), Catarina Frade, José Manuel Mendes, Luís Alçada-Almeida, Manuel Paulo Albuquerque Melo, Pedro André Ribeiro Madeira Cunha Cerqueira, Sarah Carreira da Mota

TÍTULO

Cibersegurança em Portugal: Políticas Públicas

EDIÇÃO

Faculdade de Economia da Universidade de Coimbra e CNCS

DESIGN

André Queda

FOTOGRAFIAS

pag. 0 - Freepik.com, pag. 5 - Adeolu Eletu | Unsplash, pag. 7 - Kelly Sikkema | Unsplash, pag. 9 - Joshua Hoehne | Unsplash, pag. 11 - Kaitlyn Baker | Unsplash, pag. 13 - FLY:D | Unsplash, pag. 23 - Jo Szczepanska | Unsplash, pag. 29 - Alvaro Reyes | Unsplash, pag. 43 - Ryoji Iwata | Unsplash, pag. 63 - Arthur Mazi | Unsplash, pag. 82 - Scott Graham | Unsplash, pag. 84 - ThisisEngineering RAEng | Unsplash, pag. 85 - Headway | Unsplash, pag. 86 - RoonZ | Unsplash

IMPRESSÃO

Nozzle, Lda.

TIRAGEM

120 exemplares

ÍNDICE

SUMÁRIO EXECUTIVO

O presente relatório é o primeiro publicado pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança no âmbito da sua Linha de Observação *Políticas Públicas*. No quadro da sua missão, o Observatório de Cibersegurança tem como um dos seus objetivos:

> "(...) fornecer dados para a criação de políticas públicas informadas e conscientes do estado do país nesta matéria. Ao mesmo tempo, pretende mapear as políticas que são desenvolvidas de modo a fornecer um panorama e uma comparação entre países, identificando claramente a posição de Portugal a este respeito. A linha de observação Políticas Públicas pretende dar resposta a esta necessidade."[1]

Para concretizar este objetivo foram determinadas duas tarefas. A primeira consistia num levantamento e sistematização tão exaustivo quanto possível das Estratégias e Programas Públicos nacionais relacionados com a cibersegurança. A segunda tarefa compreendia uma identificação e análise de indicadores disponíveis sobre perceções dos cidadãos na interseção entre políticas públicas e segurança do ciberespaço, indicadores esses que, não só dessem conta do panorama nacional, mas também permitissem conhecer o posicionamento de Portugal no contexto da União Europeia.

O cumprimento destas tarefas constitui o corpo principal deste *Relatório Cibersegurança em Portugal – Políticas Públicas*.

Quanto à primeira tarefa, as Secções G (Estratégias) e H (Programas Públicos) elencam e sistematizam os principais instrumentos de política pública em vigor em Portugal que contêm objetivos, atividades e metas de execução com relevância para a cibersegurança. O mapeamento realizado permitiu identificar que, para além da Estratégia Nacional de Segurança do Ciberespaço e do respetivo Plano de Ação, existe um conjunto extenso de outras estratégias, planos, programas e iniciativas nacionais (uns transversais, outros setoriais) que devem ser considerados se se pretender ter uma perspetiva mais completa e abrangente sobre o alcance das políticas públicas desta natureza em Portugal. É o caso, por exemplo, das estratégias e programas de ação associados à transição digital do país em geral e da Administração Pública em particular, bem como de instrumentos temáticos e setoriais, como a Lei de Bases da Saúde ou o Plano Nacional Energia e Clima (PNEC) 2030.

1 https://www.cncs.gov.pt/pt/observatorio/#linhasobservacao

A segunda tarefa, dedicada à análise das perceções públicas em matéria de cibersegurança, encontra respaldo na Secção I (Perceções) do relatório. Nesta secção são apresentados e analisados alguns indicadores recolhidos junto de fontes de referência, como o Eurobarómetro e o *European Social Survey,* considerados úteis para a auscultação da opinião pública sobre aspetos onde se cruzam a dimensão da cibersegurança com a das políticas públicas. Os dados recolhidos mostram que, em Portugal, tal como noutros Estados-Membros da União Europeia, existe uma divergência significativa entre a intenção dos cidadãos em reportar um eventual crime informático e o seu reporte efetivo quando são vítimas dele. Verifica-se também um elevado grau de desconhecimento sobre a existência e a identificação de canais oficiais de reporte, bem como uma preferência por canais ditos alternativos (fornecedores de Internet, por exemplo), face aos órgãos de polícia criminal. No caso particular da disseminação de notícias falsas (*fake news*), os dados mostram que os cidadãos portugueses colocam na linha da frente do combate a sua própria ação, a par com a de jornalistas e autoridades nacionais. Os resultados obtidos nesta secção proporcionam uma leitura mais rica e detalhada quando se toma em consideração algumas variáveis sociodemográficas ou se apresenta uma perspetiva comparativa com o que se passa na UE.

Este núcleo fundamental é complementado com duas secções de enquadramento do tema geral do relatório. A primeira delas (secção E) procura estabelecer um referencial teórico mínimo sobre o modo como as políticas públicas foram incorporando progressivamente as questões da cibersegurança. A segunda secção (secção F) sintetiza o quadro legal e institucional de referência em Portugal que sustenta e operacionaliza as principais Estratégias e Programas Públicos relacionados com a cibersegurança, a cibercriminalidade e a ciberdefesa. Desta síntese sobressai, por um lado, a intensificação, nos últimos anos, da produção normativa interna e europeia sobre cibersegurança e, por outro, o caráter interinstitucional e transnacional do tema, a exigir um esforço permanente de cooperação, interna e externa.

O *Relatório Cibersegurança em Portugal – Políticas Públicas* foi elaborado por uma equipa de docentes e investigadores da Faculdade de Economia da Universidade de Coimbra para o Observatório de Cibersegurança. A sua arquitetura e elaboração foi feita em estreita colaboração com o Observatório de Cibersegurança e contou com o apoio do seu Conselho Consultivo.

Agradecimentos

A equipa de docentes e investigadores da Faculdade de Economia da Universidade de Coimbra agradece os contributos dos seguintes peritos em políticas públicas e cibersegurança para o presente relatório:

Prof. Maria Manuel Leitão Marques (Eurodeputada e ex-Ministra da Presidência e Modernização Administrativa)

Dr. José Costa (*Chief Information Security Officer* da Critical Software)

Dr. Pedro Verdelho (Coordenador do Gabinete Cibercrime do Ministério Público)

Inspetor Rogério Bravo (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária)

Prof. Pedro Correia (Faculdade de Direito da Universidade de Coimbra)

B

DESTAQUES

Global Cybersecurity Index (GCI)

O *Global Cybersecurity Index* (ITU 2021) analisa cinco áreas relacionadas com a cibersegurança. Na edição de 2020, Portugal obteve a pontuação máxima em três áreas (Legal, Técnica e Cooperação), podendo ainda melhorar ligeiramente na área Organizacional e do Desenvolvimento de Capacidades. Portugal ocupa a 14ª posição no ranking mundial (42º em 2018), e a 8ª posição no ranking regional (Europa; 25º em 2018), com 97,32 pontos (em 100 possíveis).

National Cyber Security Index (NCSI)

Na última edição do *National Cyber Security Index* (E-Governance Academy 2021), Portugal obteve a pontuação máxima em 9 de 12 indicadores, incluindo o indicador sobre o desenvolvimento de políticas de cibersegurança, podendo melhorar nos indicadores Proteção de Serviços Essenciais (33/100), eID e Serviços Seguros (78/100), e Gestão de Cibercrises (60/100). Globalmente, Portugal ocupa a 4ª posição no ranking de países analisados com 89,61 pontos (em 100 possíveis), progredindo da 24ª posição que ocupava em abril de 2020.

Estratégia Nacional Segurança do Ciberespaço (ENSC) e respetivo Plano de Ação

Portugal aprovou e tem em vigor a sua Estratégia Nacional Segurança do Ciberespaço (ENSC) para o período 2019-2023, em revisão da primeira estratégia adotada em 2015. A ENSC abrange 12 objetivos que, de acordo com a ENISA[2], estão em linha com o número médio de objetivos das estratégias dos restantes países do EEE (máximo 20). O Plano de Ação associado à ENSC inclui 667 atividades programadas (2019-2021), propostas por 67 serviços e organismos da Administração Pública (em 2020). Uma percentagem muito significativa das atividades diz respeito à capacitação humana (40%) e organizacional e tecnológica (38%).

2 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

Outras estratégias e programas

A ENSC e o respetivo Plano de Ação não são os únicos instrumentos de política pública que abrangem a cibersegurança. Esta temática é também abordada em várias estratégias orientadoras de política nacional (tais como o Programa Nacional de Reformas ou a Estratégia Portugal 2030), estratégias transversais ao contexto digital (tais como a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023) e estratégias setoriais e temáticas (tais como a Lei de Bases da Saúde). Existem ainda vários programas de política pública que incluem atividades relacionadas com a cibersegurança e estabelecem metas para a sua conclusão (por exemplo, o Plano de Recuperação e Resiliência ou o Plano de Ação para a Transição Digital).

Perceção sobre a ação das autoridades públicas no combate ao cibercrime

A percentagem de cidadãos que concordam totalmente, ou tendem a concordar, que as autoridades públicas estão a fazer o suficiente nesta área tem aumentado ao longo dos últimos anos, atingindo 42% no último inquérito realizado pelo Eurobarómetro (UE 2017b).

Preocupação com o tratamento de dados pessoais

A preocupação com o tratamento de dados pelas autoridades públicas portugueses tem vindo a diminuir, mas em 2019 ainda abrangia cerca de 64% dos cidadãos segundo o Eurobarómetro (UE 2020).

Canais de reporte de cibercrimes

Existe um desconhecimento generalizado da existência de canais para reportar cibercrimes que, segundo o Eurobarómetro (UE 2020), abrange cerca de 80% da população europeia.

Intenção de reporte versus reporte atual de cibercrimes

Verifica-se uma grande discrepância entre a elevada proporção de cidadãos que têm a intenção de reportar cibercrimes caso sejam vítimas e a baixa proporção dos reportes quando são efetivamente vítimas de cibercrimes (UE 2019, 2020).

Responsabilidade pelo combate às *fake news*

Segundo o Eurobarómetro (UE 2018), existe a perceção de que o combate às *fake news* deve ser feito de igual forma pelas autoridades nacionais (45%), jornalistas (48%) e cidadãos (38%).

C

TERMOS, SIGLAS E ABREVIATURAS

ANCC	Autoridade Nacional de Certificação da Cibersegurança
AP	Administração Pública
APAV	Associação Portuguesa de Apoio à Vítima
AT	Autoridade Tributária
CCD	Centro de Ciberdefesa
CEGER	Centro de Gestão da Rede Informática do Governo
CM	Câmara Municipal
CNCS	Centro Nacional de Cibersegurança
COTEC	Associação Empresarial para a Inovação
CSIRT	*Computer Security Incident Response Team*
CSSC	Conselho Superior de Segurança do Ciberespaço
CYBERHEAD	*Cybersecurity Higher Education Database*
DGEEC	Direção-Geral de Estatísticas da Educação e Ciência
DIH	*Digital Innovation Hubs*
EEE	Espaço Económico Europeu
EMGFA	Estado-Maior-General das Forças Armadas
ENCT	Estratégia Nacional de Combate ao Terrorismo
ENESIS	Estratégia Nacional para o Ecossistema de Informação de Saúde
ENISA	Agência da União Europeia para a Cibersegurança
ENM	Estratégia Nacional para o Mar
ESS	*European Social Survey*
EUA	Estados Unidos da América
FCT	Fundação para a Ciência e Tecnologia
GNR	Guarda Nacional Republicana
GNS	Gabinete Nacional de Segurança

GO	Lei das Grandes Opções
IA	Inteligência artificial
IAPMEI	Agência para a Competitividade e Inovação, I.P.
INE	Instituto Nacional de Estatística
LBS	Lei de Bases da Saúde
MNE	Ministério dos Negócios Estrangeiros
NATO/OTAN	Organização do Tratado do Atlântico Norte
OSCE	Organização para a Segurança e Cooperação na Europa
PATD	Plano de Ação para a Transição Digital
PETI	Plano Estratégico dos Transportes e Infraestruturas
PIB	Produto Interno Bruto
PJ	Polícia Judiciária
PME	Pequenas e Médias Empresas
PNEC	Plano Nacional Energia e Clima
PNR	Plano Nacional de Reformas
PRR	Plano de Recuperação e Resiliência
PSP	Polícia de Segurança Pública
SNS	Serviço Nacional de Saúde
TIC	Tecnologias da Informação e Comunicação
UE	União Europeia
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária

D

INTRODUÇÃO

A emergência sanitária global em que vivemos desde o primeiro trimestre de 2020[3], e as suas profundas repercussões nas áreas da saúde pública, relações de trabalho e convivência social, apenas para enumerar as principais, vieram dar relevo ao papel legislador e executivo do Estado na mitigação dos vários efeitos negativos que situações extremas provocam sobre os seus cidadãos e organizações. Também a área da cibersegurança, já considerada sensível e prioritária ao ser um foco de atenção crescente por parte de várias políticas públicas, conheceu em ano e meio, nesta crise recente, um considerável agravamento das ameaças, riscos e incidentes[4], proporcional ao aumento de volume, importância e sensibilidade dos dados veiculados no ciberespaço.

Numa análise global de perceções, nos fóruns mais comuns de intervenção cívica, podemos concluir que as ações que cidadãos e organizações esperam do Estado situam-se, também, a vários níveis, tal como são várias as áreas nas quais a pandemia tem produzido os seus efeitos diretos e indiretos mais agressivos:

- no domínio da assistência aos efeitos diretos da própria doença nos cidadãos, promovendo os investimentos necessários para tornar a resposta do Serviço Nacional de Saúde (SNS) mais robusta e adequada num quadro de excecional exigência;
- no mundo empresarial, na ajuda a organizações que viram a procura dos seus bens e serviços reduzida a mínimos incompatíveis com a manutenção do regime laboral e dos postos de trabalho;
- no contexto do trabalho, com a generalização de atividades laborais deficientemente regulamentadas, feitas "à distância", e suportadas no mundo digital dos sistemas informáticos e das redes de computadores;

3 Primeiros dois casos oficiais de COVID-19 em Portugal noticiados a 2 de março de 2020.

4 Para análise mais detalhada ver *Relatório Riscos & Conflitos 2021* (CNCS 2021c). Disponível em https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf (consultado em 30/10/2021)

- na esfera individual e social, com o aumento do confinamento e isolamento de pessoas e grupos em virtude do alinhamento excecional de fatores convergentes, como sejam: os medos associados ao contágio (o próprio ou a propagação a familiares e amigos); as indicações mais ou menos vinculativas das autoridades de saúde; as dificuldades económicas que aconselham um estilo de vida caseiro de menor consumo, desencorajando o usufruto das (poucas) atividades de lazer disponíveis; e, sobretudo, o novo contexto laboral descrito nos dois pontos anteriores (quer o agravamento do desemprego, quer o aumento acentuado da modalidade remota no emprego subsistente) que obriga mais pessoas a ficar mais tempo em casa.

Todos os aspetos atrás referidos contribuem, de formas e com intensidades diferentes, para um aprofundamento do isolamento de indivíduos e núcleos familiares. Estes veem-se assim privados da inserção plena e física nos contextos sociais e profissionais, privação que, hoje se sabe, contribui negativamente para o indivíduo como um todo (aspetos psicossomáticos da saúde, situação económica, proteção legal associada a lacunas na regulamentação do novo enquadramento social e profissional predominantemente em isolamento e à distância, etc.). Como fator adicional de agravamento do risco a que o indivíduo "confinado" está sujeito, suscita-se a completa dependência deste dos meios digitais para o restabelecimento das comunicações necessárias e possíveis com o mundo exterior: para o trabalho; para a sustentação de alguma interação social; e para outras atividades pessoais do dia-a-dia mais ou menos indispensáveis à sua subsistência (compras, pagamentos, divertimento, etc.).

Este novo paradigma — "à distância" — no relacionamento entre os cidadãos/clientes e organismos da Administração Pública (AP)/empresas tem-se estendido igualmente, e de forma gradual, aos relacionamentos entre as próprias empresas/organizações entre si e, também, às interações indispensáveis entre estas e a Administração Pública Central e Local. As vantagens económicas, a comodidade e as poupanças em recursos e tempo de deslocações, associadas a este novo *modus operandi*, fazem prever que muitas das práticas tenham vindo para ficar para lá do término da emergência sanitária. Contudo, a intensificação deste novo enquadramento, potenciada pela conciliação de exigências e conveniências, tem sido, também, uma oportunidade a explorar pelos criminosos que fazem do ciberespaço o seu campo de ataque, dado o aumento drástico e contínuo que se tem verificado nas atividades que operam em modo virtual (quer em volume, sensibilidade dos dados expostos, importância económica, política, administrativa associada às transações, etc.). Constitui um desafio adicional para o Estado, no seu papel regulador, legislador, executivo e securitário, tornar (também) este espaço um local seguro para as atividades dos seus cidadãos e empresas, por exemplo, através da elaboração de políticas públicas adequadas e da monitorização dos seus efeitos. Desta forma, o Estado contribui para o desenvolvimento de uma relação de confiança na utilização dos serviços que são disponibilizados neste meio pelo setor público e privado, e que têm potenciado o desenvolvimento sustentado da sociedade.

O conteúdo do presente relatório vai ao encontro da globalidade dos objetivos enunciados neste enquadramento, assumindo-se como uma ferramenta descritiva para eventual apoio a decisões nestes domínios. Assim, são identificados vários instrumentos de política pública (estratégias, programas, iniciativas, ...) atualmente em vigor e a forma como incorporaram preocupações nos domínios associados à cibersegurança, constituindo um roteiro de fácil consulta na identificação do que já foi feito no âmbito das Políticas Públicas. São ainda analisadas as perceções dos cidadãos sobre os seus receios, a sua preparação para lidar com oportunidades, desafios e ameaças, e os seus níveis de confiança nas entidades que regulam (ou poderiam regular) aspetos relacionados com a cibersegurança, confrontando essas perceções com a realidade dos factos e as expetativas e atitudes dos próprios cidadãos.

E

GOVERNAÇÃO E CIBERGOVERNAÇÃO, CIBERSEGURANÇA E PERCEÇÃO PÚBLICA

Esta secção identifica e discute os principais conceitos associados às áreas da governação e das políticas públicas apresentando as diferentes perspetivas encontradas na literatura científica que se debruça sobre estes temas. É ainda feito o enquadramento mais restrito destes conceitos nos contextos específicos da cibergovernação[5] e da cibersegurança, analisado o papel dos destinatários últimos destas políticas (pessoas singulares e coletivas) e aferida a medida em que as suas perceções podem ter impacto na regulação do sistema.

E.1 POLÍTICAS PÚBLICAS, ESTRATÉGIAS E PROGRAMAS

A definição de política pública varia conforme os autores e as perspetivas teóricas em que estes se situam. É importante proceder a uma análise dos comportamentos e ações concretos das instituições públicas e dos seus membros, e não somente da componente formal associada aos objetivos das políticas públicas. Tal análise deve recorrer também à distinção entre os produtos (as ações formais empreendidas pelos governos para atingirem os seus objetivos) e os resultados das políticas públicas (os efeitos concretos dessas ações na sociedade) (Furlong e Kraft 2021).

5 A cibergovernação é entendida como todas as políticas, regras e procedimentos para a gestão dos riscos no ciberespaço. Uma análise aprofundada sobre os pressupostos e desafios da cibergovernação pode ser encontrada em Jayawardane *et al.* (2015).

Por uma questão de comparabilidade, e pelo facto de a arquitetura de definição e gestão das políticas públicas em Portugal se pautar, com a respetiva autonomia, pelas diretivas e orientações da União Europeia (UE), recorremos neste relatório à sua definição de política pública:

> "(...) a intervenção de uma autoridade pública, orientada por valores e finalidades, que visa uma transformação da sociedade a médio e longo prazo, com recurso a diversos meios de ação. Uma política pública é aplicável no território em que é competente a autoridade que a leva a cabo" (UE 2021b)

Tal definição reflete a relevância do planeamento estratégico que, incorporando mais recentemente as questões territoriais, ambientais e da sustentabilidade, é o suporte epistémico e conceptual das políticas públicas na União Europeia e nos seus Estados-Membros.

Tal acentua também a importância de se atender aos processos de territorialização referentes às políticas públicas sobre cibersegurança, criando o desafio e a necessidade de uma definição precisa da escala de aplicação das medidas a implementar na definição da cidadania digital.

A filosofia e a dinâmica concreta de atuação da União Europeia podem ser vistas na atualidade como uma experiência de governação não hierárquica, de articulação público-privada e deliberativa, que releva as questões normativas e de legitimidade democrática, regida pelo intergovernamentalismo (Morillas 2020; Pollack 2015).

Os Tratados europeus e a lógica de avaliação das políticas públicas consagraram uma arquitetura hierárquica de planeamento estratégico com as seguintes dimensões:

- Estratégia: com especificação dos eixos estratégicos;
- Plano: associado aos eixos de intervenção;
- Programa: com definição de linhas de ação;
- Ações e atividades: que constituem o plano operacional da estratégia, adequadamente calendarizado.

A União Europeia consensualiza o conceito de estratégia a nível europeu com a seguinte definição:

> "(...) orientações políticas e domínios prioritários para as ações da UE a longo prazo que são utilizadas como base do Programa de Trabalho da Comissão e das iniciativas legislativas e não legislativas" (UE 2021a).

Tal definição é transponível para o âmbito nacional de cada Estado-Membro da UE, refletindo as estratégias e as prioridades do governo a médio prazo, procurando dar coerência à ação coletiva de todos os ministérios de uma dada área de intervenção.

A UE, devido à latitude de ação dos governos nacionais que a compõem, não propõe definições consensualizadas de Plano ou de Programa. No contexto da governação pública em Portugal, consolidou-se nos últimos anos uma nomenclatura que consiste nas seguintes conceções:

- Plano de ação: procura articular as diversas sinergias e políticas setoriais, sendo definido a nível governamental e especificando as responsabilidades e competências dos diversos atores participantes, permitindo também a programação de ações a implementar.
- Programa: ações e atividades para operacionalizar uma linha de ação e é definido por uma entidade pública específica. Esta entidade congrega e articula as atividades e ações concretas realizadas por diferentes entidades públicas e privadas.

Esta nomenclatura serve de base à estruturação do presente relatório. Cabe referir que a definição estratégica e a consecução dos objetivos definidos é um processo dinâmico, sendo necessário um equilíbrio consequente entre os objetivos estratégicos (*ends*), as diferentes alternativas para os atingir (*ways*) e os recursos existentes (*means*). O não alinhamento ou falta de equilíbrio entre estes três fatores aumenta o risco de não concretização das estratégias (Holcomb, 2004).

E.2 CIBERSEGURANÇA, GOVERNAÇÃO E POLÍTICAS PÚBLICAS

De uma forma geral, podemos distinguir duas formas de cibergovernação:

- Cibergovernação baseada na conformidade e na observância das regras: baseada no reporte obrigatório de falhas e quebras de segurança e enquadramento das práticas em legislação específica.
- Cibergovernação baseada na reputação e na acreditação: assente em mecanismos de garantia baseados nas boas práticas e em padrões auditados e consensualizados (Bossomaier, D'Alessandro, e Bradbury 2020).

Vários países (Austrália, EUA, Reino Unido, Nova Zelândia, Canadá, China e Índia), bem como a União Europeia, centram a lógica de regulação do ciberespaço e a cibersegurança na proteção dos dados individuais e nas quebras de segurança. Contudo, alguns especialistas consideram mais importante fomentar lógicas de autorregulação com a adoção de quadros de boas práticas e/ou de acreditação (Burdon, Lane, e von Nessen 2012; Manjikian 2021).

A proposta mais sólida e coerente de análise sobre políticas públicas de governação do ciberespaço ou de cibergovernação na UE, numa perspetiva mais abrangente, foi avançada por Mirela Mărcuţ (2020). Segundo esta autora, a cibergovernação na UE pode ser analisada a partir de dois quadros analíticos: a governação experimentalista e a governação multinível.

A governação experimentalista, sobretudo no que concerne à cibergovernação, é relevante porque acentua a "aprendizagem através da prática" e a relação entre a UE e os Estados-Membros. A governação multinível inclui as entidades nacionais e regionais no ciclo de governação, mas dá a devida ênfase à autonomia do nível supranacional e ao papel da UE como um ator de pleno direito e com uma capacidade de atuação independente em relação aos Estados-Membros.

E.3 POLÍTICAS PÚBLICAS E CIBERSEGURANÇA: AS DIFERENTES DIMENSÕES TEÓRICAS E ANALÍTICAS

A questão da cibersegurança não se reduz a uma componente técnica, estando a sua complexidade relacionada com as políticas públicas na área da economia, da inovação, das liberdades civis e das relações internacionais e da segurança nacional (Clark, Berson, e Lin 2014; Walton *et al*. 2021).

As políticas públicas de cibersegurança estão diretamente relacionadas com o nível de desenvolvimento científico e técnico de um país, e menos com as ameaças externas à segurança, a política interna ou a sua cultura política (Calderaro e Craig 2020).

A análise da cibersegurança a nível interestatal pode ser efetuada a partir de um quadro analítico baseado no risco e na incerteza (Brantly 2021). Constata-se que a maior parte da legislação existente é produzida por representantes dos Estados, não atendendo diretamente a outro tipo de atores presentes no ciberespaço e relevantes para as questões de cibersegurança (Katagiri 2021).

Para uma análise consistente da política de cibersegurança, fundamentando a escolha de indicadores pertinentes, podem-se identificar as seguintes esferas de influência: a tecnológica, a política, e a societal.

Os fatores impulsionadores (*drivers*) são:

- a política internacional e a política interna (esfera política);
- a institucionalização e os debates académicos (esfera societal);
- os acontecimentos relevantes, tanto no âmbito da cibersegurança como fora do mesmo, e o desenvolvimento e utilização das tecnologias digitais (esfera tecnológica) (Dunn Cavelty e Wenger 2020).

A validação de indicadores para o estudo da cibersegurança pode ter uma valência qualitativa ou quantitativa. A nível qualitativo, pode-se recorrer a peritos e à ativação de técnicas de análise específica, como a análise temática e a análise de redes (*network analysis*), definindo os parâmetros da cibersegurança e do risco na cibersegurança (Cains *et al*. 2021).

A nível quantitativo existe um conjunto de trabalhos e propostas que se centram na definição de índices ou indicadores. Entre os mais conhecidos e utilizados, existe o *Global Cybersecurity Index* (GCI) da ONU/ITU, muito bem estruturado e fundamentado a nível conceptual, analítico e de operacionalização, tendo por objetivo a comparação a nível de países (ITU 2021). Este índice tem cinco pilares analíticos fundamentais: medidas legais, medidas técnicas, medidas organizacionais, medidas de capacitação e medidas de cooperação. Os cinco pilares têm componentes associadas diretamente a políticas públicas específicas.

Podemos identificar outras propostas de definição de indicadores, ainda que possam não ter originado índices de cibersegurança de utilização global:

- o estudo da RAND sobre a construção de uma métrica para a cibersegurança e a ciber-resiliência (Snyder *et al*. 2020);
- a análise da Avaliação do Impacto Societal (*Societal Impact Assessment* – SAI) e a elaboração de uma matriz, a partir da metodologia da cocriação. A matriz é composta por cinco níveis analíticos: societal, individual, comunitário, disseminação e comunicação (Aaltola e Ruoslahti 2020).
- o estudo do impacto dos fatores socioestruturais, uma vez que o Produto Interno Bruto (PIB) e o grau de preparação global de um país (medido pelo *Global Cybersecurity Index* - GCI) são os melhores preditores para a preparação dos indivíduos a nível da cibersegurança. Daí a importância das medidas governamentais para a promoção da cibersegurança (Lee e Kim 2020).

A nível quantitativo há um vasto leque de estudos sobre as perceções do risco associadas à cibersegurança. Especial relevância deve ser dada aos comportamentos micro dos indivíduos e à sua relação com eventuais medidas de políticas públicas para a cibersegurança (Kostyuk e Wayne 2021). O papel da desinformação digital emerge como fulcral na definição de políticas públicas de cibersegurança, dado que esta afeta de forma direta a resiliência dos cidadãos (Bârgăoanu e Radu 2018)[6].

6 Cabe referir a nível das políticas públicas o Plano de Ação contra a Desinformação [JOIN/2018/36 final].

Especificamente sobre o caso português, alguns autores referem a existência de um desfasamento e de um enviesamento conjuntural das perceções no sentido de uma apreciação pouco objetiva da gestão pública e das políticas públicas em cibersegurança e cibercrime (Correia, Santos, e Bilhim 2017). Ou seja, os estudos realizados indicam que os portugueses se encontram globalmente pouco satisfeitos com a ação do Estado em matérias de cibersegurança e cibercrime, o que contrasta com a perceção positiva em relação à segurança dos dados e familiarização, à tecnologia e monitorização de atividades, e à confidencialidade e uso indevido dos dados.

Sobre as perceções em relação à ação do Estado em matéria de cibersegurança, emergem alguns tópicos relevantes para a ação do Estado e para as políticas públicas: confidencialidade e segurança; tecnologias e consciencialização; e ação do Estado (Correia e Santos 2018).

E.4 POLÍTICAS PÚBLICAS E CIBERSEGURANÇA: COMPONENTE TÉCNICA E FORMAS DE AVALIAÇÃO

Ao nível da União Europeia e dos recursos e meios instalados relevantes para a cibersegurança, a Agência da União Europeia para a Cibersegurança (ENISA) publicou um quadro de avaliação bastante detalhado, permitindo aos Estados-Membros um diagnóstico rigoroso sobre a sua situação (Sarri *et al*. 2020). O Quadro de Avaliação proposto consiste em 17 objetivos estratégicos agrupados em quatro núcleos temáticos, tal como consta da Figura 1.

Figura 1. Núcleos temáticos do Quadro de Avaliação proposto pela ENISA

Especificamente para a temática do conhecimento e da sensibilização (*awareness*) em cibersegurança, o delinear de políticas públicas eficazes depara-se com os seguintes obstáculos: visibilidade limitada, complexidade sociotecnológica, impactos ambíguos e o caráter não consensual do combate à cibersegurança (de Bruijn e Janssen 2017).

A avaliação comparativa (*benchmarking*) de cibersegurança, baseada na análise às políticas e práticas de 37 países (Portugal não está incluído), resultou na identificação de sete modelos (Bahuguna, Bisht, e Pande 2020) que influenciaram e estão na origem de alguns dos índices globais mais proeminentes. Os modelos identificados são os seguintes:

- *Cyber Index – United Nations* (ONU 2013): esteve na base da criação do *Global Cybersecurity Index* (ITU 2021) e de outros índices com menor relevância pública promovidos por um dos autores do relatório;
- *Community Cybersecurity Maturity Model* (CCSMM): modelo de maturidade criado pelo *Center for Infrastructure Assurance and Security* (CIAS) *at The University of Texas at San Antonio*[7] (White 2011);
- *Cyber Readiness Index*[8] (Hathaway 2015);
- *National Cybersecurity Maturity Model* (NCSecMM) (el Kettani e Debbagh 2008);
- *Global Cybersecurity Index (GCI)* & *Cyberwellness Profiles* (ITU e ABIresearch 2015): se no relatório de 2015 as duas dimensões (*cybersecurity* e *cyberwellness*) eram analisadas em conjunto, atualmente autonomizou-se e ganhou proeminência o *Global Cybersecurity Index (GCI)* (ITU 2021);
- *National Information Security Index* (Korea Internet & Security Agency 2008);
- *Cyber Power Index* (Economist Intelligence Unit e Booz Allen Hamilton 2011).

Para além dos índices e modelos de maturidade acima referidos, destaca-se ainda atualmente o *National Cyber Security Index* enquanto índice global de medição do grau de preparação dos países para prevenir ciberameaças e gerir ciberincidentes (E-Governance Academy 2021).

No que diz respeito às competências da população em geral quanto à cibersegurança, o nível de conhecimento e de sensibilização dos utilizadores e o nível de boas práticas em cibersegurança dependem das fontes a que recorrem para se orientarem. Daí o relevo de políticas públicas de cibersegurança claras e objetivas e de instrumentos de informação disponíveis para o público em geral de acesso fácil e baseados na evidência científica e técnica, rigorosos e bem estruturados (Holton e Furnell 2020).

E.5 PERCEÇÃO E POLÍTICA PÚBLICA EM CIBERSEGURANÇA

A convivência numa sociedade democrática estimula o exercício da "opinião pública", e esta, por sua vez, participa de forma relevante na regulação da própria sociedade, ao ser alvo de uma atenção crescente por parte dos gestores e dos decisores políticos (Obiam 2021; Wlezien e Soroka 2016). Os canais cada vez mais eficientes de disseminação de informação, a sua grande abrangência, e o acesso fácil do cidadão comum a muitos deles, tanto para receber como para colocar informação (como são exemplos as redes sociais, os canais de TV e rádio locais e nacionais), tornam quase incontornável a consideração deste manancial informativo na gestão política e administrativa das sociedades.

7 https://cias.utsa.edu/the-ccsmm.html
8 https://www.potomacinstitute.org/academic-centers/cyber-readiness-index

É assim factual que a informação chega atualmente ao cidadão comum em considerável diversidade e quantidade. Mas cumprirá avaliar a conceção que este faz dela, analisando-se em que medida a capta e como a interpreta, se consegue identificar os seus diferentes níveis de rigor e precisão, bem como as intenções por detrás da sua divulgação[9], como ela condiciona as suas opiniões e atitudes e como cada um contribui para a sua (re)divulgação (e o grau de adulteração associado a estes processos de intermediação). Esta é a função global dos estudos de opinião. As análises dos seus resultados (individualizados, em séries espaciais e/ou temporais, deteções de padrões, interações e dependências entre conjuntos) e das suas condicionantes atrás referidas são, cada vez mais, tidas em conta pelos decisores políticos na sua ação reguladora (Burstein 2020).

No universo informativo globalizado, alguns temas têm merecido um crescente interesse por parte dos cidadãos. Temas como o ambiente sustentável e as diferentes vertentes da discriminação de pessoas e grupos têm merecido uma grande cobertura mediática e sido objeto de inúmeros estudos científicos nas áreas da sociologia, ciência política e economia, que procuram a racionalidade das mudanças políticas. Outros temas críticos como as políticas fiscais, de defesa ou de gestão de infraestruturas, não merecem habitualmente tanta atenção dos cidadãos e, talvez por isso, não sejam alvo da mesma cobertura mediática, nem de tantos estudos científicos e/ou de opinião (Wlezien e Soroka 2016). Outros temas clássicos têm merecido um justificado aumento acentuado de relevância, motivado pelas recentes crises económicas e sanitárias. É o caso do papel do Estado, por exemplo, na proteção social, no apoio ao setor privado, na prestação de cuidados de saúde e na proteção dos dados de cidadãos e empresas que, cada vez mais, circulam num espaço virtual que apresenta défices de regulamentação e problemas de segurança[10].

Havendo alguma controvérsia entre autores sobre o grau de determinismo no impacto da opinião pública sobre a elaboração de políticas, nomeadamente nas que se (re)aplicam à esfera pública (realimentando, com elevada probabilidade, a própria opinião pública), a relevância deste impacto é um dado objetivo globalmente aceite pela comunidade científica que se dedica a este estudo. Alguns autores, contudo, consideram outros atores[11] como igual ou superiormente decisivos (Burstein 2020).

O acesso à opinião pública faz-se, normalmente, pela auscultação da informação em "domínio público", através do planeamento de instrumentos de medição, recolha e posterior análise estatística das perceções, das formulações de opinião, e das atitudes e reações dos cidadãos relativamente aos aspetos em análise. É um papel básico das democracias representativas criar plataformas de suporte à intervenção da opinião pública (objetiva) dos seus cidadãos (Obiam 2021), nas quais a contagem de votos nas diversas eleições será a única e/ou derradeira instância. O sistema democrático deve também exercer um papel regulatório para evitar a preponderância excessiva de grupos, setores, fações, correntes, "formadores de opinião" (*opinion makers*), etc. Deve ainda promover a educação e formação adequadas e isentas dos seus cidadãos, contribuindo para o desenvolvimento do discernimento individual, arma eficaz para atenuar os efeitos negativos das diferentes estratégias de desinformação, como as "notícias falsas" (*fake news*), por exemplo.

9 Estas podem ser as mais variadas, desde os previsíveis e facilmente detetáveis intuitos formativos ou comerciais, a ações mais ou menos coordenadas e direcionadas de desinformação que podem ter uma interferência grave na aferição da opinião pública "genuína e estável" e afetar, de forma indesejável e inadequada, os processos onde essa aferição é utilizada.

10 Para análise mais detalhada ver *Relatórios Ética & Direito 2020* (CNCS 2020c) e *Relatório Riscos & Conflitos 2021* (CNCS 2021c).

11 É o caso de organizações não governamentais, grupos de pressão, organizações políticas, sociedades de advogados, etc.

Alguma correlação entre opinião e política pública, em cada domínio da atividade política, é, assim, essencial, numa democracia representativa. Não é por isso estranho que diversos estudos científicos tenham analisado esta correlação entre ambas, procurando formular diferentes modelos onde as políticas são consideradas como funções das opiniões (estas últimas tidas como variáveis independentes) (Wlezien e Soroka 2016). A dificuldade maior destes estudos centra-se, precisamente, neste ponto: isolar as diferentes opiniões públicas (seus determinantes e efeitos) de todo o restante conjunto de variáveis, i. e., formar variáveis efetivamente independentes. Não será sempre possível contornar esta dificuldade de forma significativa e, muitas vezes, nem de forma controlável (os efeitos cruzados podem não ser quantificáveis). A opinião pública pode ser parcialmente baseada em informação "publicamente disponível":

- desde displicentemente pouco rigorosa a intencionalmente falsa;
- influenciada por más políticas prévias nas mesmas áreas;
- ou pode resultar de crises conjunturais sociais, económicas, sanitárias, resultantes da intensificação de medos, tensões, ódios, etc. (justificados, ou não; espontâneos e genuínos ou induzidos de forma deliberada, artificiais e efémeros).

Mesmo considerando estas limitações, existem aspetos de extrema relevância a ponderar na elaboração de políticas públicas: a extensão, abrangência e precisão dos factos que o público conhece nos domínios-alvo; a qualidade da informação que consegue extrair desses factos; e as diferentes linhas de opinião que formula nos diferentes contextos relacionados.

Se estas asserções são óbvias quando nos focamos em domínios específicos — como os da conceção, fabrico e comercialização de produtos — onde gestores podem intervir, por exemplo, definindo estratégias de *marketing*, são igualmente válidas no domínio das políticas públicas em contextos como o da cibersegurança, onde os responsáveis de topo podem intervir com a elaboração de políticas públicas específicas integrando diferentes objetivos (normativos, incentivos, punitivos, informativos, preventivos, ...).

A perceção pública constitui, assim, uma fonte fundamental de indicadores relevantes:

- na avaliação de aspetos que possam não estar a ser geridos, ou comunicados, da forma mais adequada à comunidade de interessados (monitorização e reavaliação de políticas públicas);
- na identificação de problemas novos, fraturantes, ou ainda não tratados, que a comunidade de interessados considera de intervenção necessária e/ou urgente (elaboração de políticas públicas).

Ainda no contexto das perceções, justifica-se uma referência a estratégias de desinformação e ao fenómeno das *fake news* dado o aumento do seu impacto global, nos últimos anos, em diferentes áreas da atividade humana (incluindo na área política e em áreas relacionadas com a cibersegurança).

O fenómeno das *fake news* não é novo, uma vez que a publicação de informação falsa, rumores, manipulação, desinformação e teorias da conspiração, existe desde que o ser humano começou a comunicar. De facto, cada nova tecnologia de comunicação tem permitido novas maneiras de manipular e ampliar a desinformação para as pessoas e sociedades (Burkhardt 2017). Sendo a veracidade da informação, de um modo geral, difícil de confirmar, e, uma vez comunicada ao público global, difícil de corrigir de forma efetiva, as sucessivas "novas tecnologias" (imprensa escrita, rádio, TV, Internet, redes sociais) possibilitaram um agravamento do fenómeno ao potenciar uma disseminação muito mais rápida, em maiores quantidades e a palcos mais abrangentes com pouca ou nenhuma supervisão editorial.

Destacaram-se dois eventos históricos onde, apesar de terem sido difundidos como entretenimento, o tom noticioso dos mesmos causou pânico entre os ouvintes:

- a emissão de Ronald Knox em 1926 através da BBC do programa "*Broadcasting the Barricades*", que relata uma suposta invasão comunista de Londres;
- a emissão de Orson Wells, "*War of the Worlds*", em 1938 sobre uma suposta invasão marciana dos EUA.

Como referido por Wall (2015), as novas tecnologias permitem a não-jornalistas alcançar uma vasta audiência. Assim, são necessárias novas formas de enfrentar os desafios impostos pelas *fake news* em comparação com as exigidas pelas tecnologias de comunicação anteriores. Além disso, as consequências intencionais e não intencionais das mesmas aumentaram exponencialmente. Neste contexto, assistimos nos últimos anos a fenómenos internacionais bem conhecidos do público em geral, onde a utilização massiva de *fake news* (bem como da acusação de falsidade de notícias verdadeiras) atingiu tal impacto na manipulação da opinião pública que colocou este problema na agenda internacional (Quandt *et al.* 2019). O desenvolvimento de algoritmos de *machine learning*, uma área da Inteligência Artificial, veio ainda possibilitar que o fenómeno das *fake news* não se limitasse à criação de conteúdos falsos na forma escrita. Atualmente estes algoritmos possibilitam também a manipulação e geração de conteúdo áudio e vídeo falso (*deep fakes*), reforçando a sua credibilidade junto do público em geral e tornando ainda mais difícil a deteção da falsificação.

No caso concreto do triângulo "perceção/política pública/cibersegurança", o acesso à informação e às opiniões em "domínio público" pode ter em vista diferentes metas, tais como:

1. avaliar diferentes prioridades de intervenção do Estado na abordagem a problemas já identificados pelas populações ou pelas próprias autoridades do Estado, bem como avaliar a eficácia das medidas já tomadas para os mitigar;
2. identificar novos problemas relevantes que ainda não mereceram atenção por parte de políticas específicas;
3. avaliar a eficácia das estratégias de comunicação utilizadas na divulgação de políticas prévias e dos seus resultados, bem como avaliar os resultados das ações de formação, divulgação, e prevenção, conducentes à mitigação dos riscos, impactos e generalização do cibercrime;
4. aferir da correlação entre aquilo que o público perceciona e o que efetivamente caracteriza a realidade em termos de cibersegurança (ou falta dela), i.e., ver até que ponto as sensações de segurança, medo, confiança em sistemas e entidades, etc., são justificadas pelo volume, gravidade, impacto económico e social, dos episódios registados neste contexto;
5. avaliar a preparação do público para identificar os vários tipos de ameaça, caracterizando assim o quadro global de vulnerabilidade dos cidadãos relativamente ao cibercrime, e, simultaneamente, tipificar as várias formas de resposta dos cidadãos às ameaças por eles identificadas e os seus níveis de confiança nas entidades que monitorizam e combatem o cibercrime, projetando os efeitos a médio prazo das intervenções no campo da informação/formação dos cidadãos e da proteção dos sistemas e redes;

6. e perceber, ainda, em que medida todos estes dados objetivamente aferidos através de indicadores específicos, são afetados por fenómenos adversos (no que respeita à qualidade e abrangência da informação circulante), como as *fake news*, diferentes tipos de censura, restrições de acesso às redes, etc. Estes fenómenos podem ter impacto significativo nas perceções que, globalmente, podem interferir com a elaboração de políticas públicas. Estas, por sua vez, podem ser usadas para potenciar a cibersegurança e combater a desinformação.

Este relatório procura contribuir para os seis objetivos atrás referidos a propósito do processo de elaboração de políticas públicas no domínio da cibersegurança.

F

QUADRO INSTITUCIONAL E LEGAL DA ESTRUTURA NACIONAL DE CIBERSEGURANÇA

A cibersegurança, entendida como política pública, possui uma natureza transversal, permeando as mais diversas políticas públicas setoriais, onde o processo de transição digital está em marcha acelerada e, consequentemente, os riscos e ameaças à segurança das redes e sistemas de informação se intensificam e colocam maiores desafios às entidades que os utilizam para o cumprimento das respetivas atividades. As estratégias, programas e ações no domínio da cibersegurança que povoam as políticas públicas em Portugal encontram fundamento num conjunto de dispositivos legais e regulamentares próprios que constituem o quadro normativo de referência para a elaboração e efetivação de uma política de segurança do ciberespaço[12]. A ele se associa uma componente institucional que é responsável pelo desenho, execução, monitorização e fiscalização do cumprimento desse quadro normativo fundamental.

A integração de Portugal na UE, bem como em organizações internacionais como a NATO e a OSCE, justifica que o essencial do panorama jurídico-político nacional em matéria de cibersegurança surja como consequência das medidas adotadas e compromissos assumidos no contexto das organizações de que é membro. De igual forma, a estrutura institucional interna abre-se também à articulação com atores externos, criando uma prática de interações transnacionais imprescindível quando se trata de lidar com uma realidade que não se circunscreve a fronteiras nacionais. De facto, o caráter transnacional das ciberameaças, a par do elevado grau de interdependência das economias nacionais, tornam muitas vezes uma ação individual e isolada dos Estados insuficiente ou pouco eficaz. Consequentemente, a cooperação internacional torna-se um imperativo para a prevenção e resolução de incidentes, e para a construção de um ciberespaço mais seguro numa sociedade cada vez mais digital.

12 A recém-aprovada *Carta Portuguesa de Direitos Humanos na Era Digital* (Lei n.º 27/2021, de 17 de maio, retificada pela Declaração de Retificação n.º 18/2021, de 9 de junho) inclui, no seu art. 15.º, o *Direito à cibersegurança,* impondo ao Estado o dever de definir políticas públicas que garantam a proteção dos cidadãos e das redes e sistemas de informação.

Nesta secção apresentam-se os diplomas principais que contêm a arquitetura legal e institucional da cibersegurança em Portugal, incluindo em domínios especialmente relevantes como a ciberdefesa e o combate à cibercriminalidade (secções F.1., F.2. e F.3.). Neles se sustentam muitas das estratégias e iniciativas ligadas à segurança do ciberespaço que são destacadas no presente relatório, bem como o fundamental da estrutura institucional. De forma complementar, é feita uma breve referência aos principais interlocutores externos das instituições nacionais, no quadro da cooperação transnacional naqueles mesmos domínios relevantes (secção F.4.).

F.1 CIBERSEGURANÇA

A Lei n.º 46/2018, de 13 de agosto, estabelece o *Regime Jurídico da Segurança do Ciberespaço*, transpondo para a ordem jurídica interna a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 (Diretiva SRI). A Diretiva SRI constitui a primeira medida legislativa ao nível da UE destinada a reforçar a cooperação entre Estados-Membros no que respeita à cibersegurança, estabelecendo nomeadamente obrigações de segurança a cumprir pelos operadores de serviços essenciais em setores críticos como transportes, energia, saúde, finanças, assim como pelos prestadores de serviços digitais. Desde maio de 2019, existe também no âmbito do Conselho da UE um quadro de sanções aplicáveis a pessoas ou entidades associadas a casos específicos de ciberataques com origem no exterior da UE que constituam uma ameaça à União ou aos seus Estados-Membros[13].

Encontra-se atualmente em preparação uma nova diretiva – *Diretiva SRI 2* – para responder à evolução do cenário de ciberameaças. Entre outras medidas, prevê-se que a nova Diretiva SRI 2 venha reforçar o regime de obrigações das empresas em matéria de segurança, intensificar a partilha de informação e a cooperação entre Estados-Membros, e tornar mais rigorosa a supervisão das autoridades nacionais.

A Lei nº 46/2018 define as bases jurídicas e institucionais da cibersegurança em Portugal, mas somente para o âmbito civil. Esta lei é aplicável à Administração Pública (AP), aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a quaisquer entidades que utilizem redes e sistemas de informação, nomeadamente no âmbito da notificação voluntária de incidentes. De fora ficam as entidades que operam as redes e sistemas de informação militares (diretamente relacionados com o EMGFA e com qualquer ramo das Forças Armadas) e de informação classificada (art. 2º da Lei n.º 46/2018).

O diploma apresenta um elenco de conceitos e noções próprios do ciberespaço (por exemplo, "incidente", "infraestrutura crítica", "norma", "prestador de serviços digitais", "segurança das redes e dos sistemas de informação", entre outros), que delimitam as responsabilidades e obrigações dos diferentes atores e entidades nele envolvidos (art. 3.º).

Confere ao Governo a competência para elaborar e aprovar a Estratégia Nacional de Segurança do Ciberespaço (ENSC), a qual define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional (art. 4º). A Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, aprovou a ENSC 2019-2023, sucedendo à Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, que aprovou a primeira ENSC.

13 https://www.consilium.europa.eu/pt/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

A mesma Lei fixa ainda a estrutura de segurança do ciberespaço em Portugal, que compreende o Conselho Superior de Segurança do Ciberespaço (CSSC), o Centro Nacional de Cibersegurança (CNCS) enquanto Autoridade Nacional de Cibersegurança (que funciona no âmbito do Gabinete Nacional de Segurança – GNS) e a Equipa de Resposta a Incidentes de Segurança Informática (CERT.PT)[14]. Os operadores de serviços essenciais (energia, água, transportes, banca e infraestruturas do mercado financeiro, saúde e infraestruturas digitais) e os prestadores de serviços digitais completam a lista, cabendo-lhes, entre outros, o dever de proceder à notificação da respetiva atividade junto do CNCS.

Recentemente, o Decreto-Lei n.º 65/2021, de 30 de julho, veio regulamentar o Regime Jurídico da Segurança do Ciberespaço aprovado pela Lei n.º 46/2018, nos aspetos relativos à definição dos requisitos de segurança das redes e sistemas de informação e das regras para a notificação de incidentes por parte da Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. O decreto-lei estabeleceu ainda as obrigações em matéria de certificação da cibersegurança, em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, permitindo a implementação de um quadro nacional de certificação da cibersegurança pelo CNCS que, por isso, se assume como a Autoridade Nacional de Certificação da Cibersegurança (ANCC). Nessa qualidade, o CNCS integrará o Grupo Europeu para a Certificação da Cibersegurança (GECC), previsto no art. 62º do Regulamento (UE) 2019/881[15].

F.2 CIBERCRIME

A Lei n.º 109/2009, de 15 de setembro é o diploma que aprova a *Lei do Cibercrime*, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho da UE, de 24 de fevereiro, relativa a ataques contra sistemas de informação. Além disso, adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, aprovada em Budapeste a 23 de novembro de 2001 (aprovada pela Resolução da Assembleia da República n.º 88/2009, de 10 de julho de 2009 e ratificada pelo Decreto n.º 91/2009, de 15 de setembro). A Lei n.º 109/2009 revogou a Lei n.º 109/1991, de 17 de agosto, denominada *Lei da Criminalidade Informática*.

A Lei do Cibercrime procura reunir num único diploma todas as normas respeitantes à criminalidade informática[16]. Inclui normas de direito substantivo (tipologia de cibercrimes), normas de direito processual (designadamente sobre recolha e conservação de prova digital) e normas relativas à cooperação judiciária internacional em matéria penal.

14 Artigos 5º a 11º da Lei n.º 46/2018, de 13 de agosto. Para maiores desenvolvimentos sobre a composição e competências do CSSC, do CNCS e do CERT.PT ver *Relatório Ética & Direito 2020* (CNCS 2020c).

15 O Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, veio conferir um mandato permanente à ENISA e fixar os seus objetivos, atribuições e aspetos organizativos. Veio, igualmente, enquadrar a criação dos sistemas europeus de certificação da cibersegurança de produtos e serviços digitais, bem como proceder à revogação da anterior Lei da Cibersegurança europeia, aprovada pelo Regulamento (UE) 526/2013, de 21 de maio de 2013.

16 No entanto, esta lei não esgota todos os tipos legais de criminalidade informática. Como se pode ler no ponto 1 da Estratégia Nacional para a Segurança do Ciberespaço 2019-2023 (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho), por "cibercrime entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa."

Na estrutura institucional de combate ao cibercrime, destacam-se o *Gabinete Cibercrime* do Ministério Público e a *Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária* (UNC3T)[17]. Enquanto Autoridade Nacional de Cibersegurança, o CNCS mantém com estas entidades uma articulação e cooperação estreita no âmbito do combate à criminalidade informática e no ciberespaço.

F.3 CIBERDEFESA

A Lei de Defesa Nacional (Lei Orgânica n.º 1-B/2009, de 7 de julho) determina, no seu art. 7º, que é responsabilidade conjunta da Assembleia da República e do Governo definir as grandes opções do Conceito Estratégico de Defesa Nacional (CEDN), que serão aprovadas por resolução do Conselho de Ministros (presentemente vigora a Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril). Entre os aspetos fundamentais a ter em conta na estratégia global a adotar pelo Estado para a concretização dos objetivos da política de segurança e defesa nacional, o CEDN em vigor desde 2013 identifica a cibercriminalidade e o ciberterrorismo como ameaças e riscos tanto à segurança global, como nacional. Cabe ao EMGFA planear, dirigir e controlar a ciberdefesa (Lei Orgânica de Bases da Organização das Forças Armadas nº 2/2021, de 9 de agosto 2021).

Pressupondo uma articulação e cooperação tanto à escala nacional (designadamente com o CNCS e com os órgãos de polícia criminal) como internacional (com a NATO e a UE, em particular), foi criado, no âmbito do EMGFA, o Centro de Ciberdefesa (CCD) para agilizar essa articulação institucional e dar corpo às iniciativas de ciberdefesa (art. 31º, do Decreto-Lei n.º 184/2014, de 29 de dezembro).

Compete ao CCD dirigir e coordenar a capacidade nacional de ciberdefesa, incluindo conduzir operações militares no ciberespaço e proteger os sistemas de informação das Forças Armadas (art. 45º do Decreto Regulamentar n.º 12/2015, de 31 de julho). Na sua atuação, estão também compreendidas atividades de formação, treino, investigação de ciberincidentes e cooperação internacional.

O trabalho do CCD é executado em estreita colaboração com o CNCS, com o qual partilha informação na perspetiva de respostas defensivas. Nesse sentido, a articulação e a partilha de informação do CCD com o CNCS, com os *Computer Incident Response Capability* (CIRC) nacionais e internacionais e com outras entidades com responsabilidades na gestão e fiscalização do ciberespaço servem para a consolidação de uma estratégia de resposta nacional às ciberameaças.

F.4 RELAÇÕES INSTITUCIONAIS DE ÂMBITO TRANSNACIONAL

Como referido no início desta secção, as capacidades nacionais em matérias de cibersegurança, cibercrime e ciberdefesa articulam-se com as de organizações internacionais das quais Portugal é membro, como é o caso da UE, da NATO e da OSCE. É, por isso, oportuna uma referência breve às principais relações institucionais que se verificam no quadro dessas organizações.

17 Relativamente à composição e competências do Gabinete Cibercrime do MP e do UNC3T da PJ ver *Relatório Ética & Direito 2020* (CNCS 2020c). De notar que, por força da entrada em vigor, a 1 de janeiro de 2020, do novo Estatuto do Ministério Público (Lei nº 68/2019, de 27 de agosto) e nos termos da Deliberação do Conselho Superior do Ministério Público de 20 de outubro de 2020, o Gabinete Cibercrime deixou de ser uma estrutura informal da Procuradoria-Geral da República para se tornar o gabinete de coordenação nacional na área do cibercrime.

Um dos principais pilares da cooperação internacional no campo da cibersegurança assenta na relação do CNCS com a Agência da UE para a Cibersegurança (ENISA)[18]. Enquanto ponto focal da cooperação europeia, a ENISA coordena e sincroniza a cooperação operacional e técnica entre todos os atores que, no espaço da UE, colaboram para responder a incidentes e crises de larga escala. Em conjunto, estes atores constituem a rede europeia de CSIRT (*Computer Security Incident Response Team*), chamada CSIRT-EU.

A Rede Europeia CSIRT-EU (*Computer Security Incident Response Team*), estabelecida pela Diretiva (UE) 2016/1148 (Diretiva SRI), é constituída por equipas de resposta rápida a incidentes de segurança informática de entidades públicas e privadas que operam nos Estados-Membros[19]. O CERT.PT é o representante de Portugal nesta rede europeia, além de integrar a própria Rede Nacional CSIRT[20,21].

A CyCLONe é a Rede de Organização de Ligação para Crises do Ciberespaço da UE[22]. Foi criada em 2020 no âmbito do Programa HORIZON 2020, tendo como objetivo contribuir para a implementação do Plano da Comissão Europeia para uma resposta de emergência rápida em caso de incidente ou crise cibernética em grande escala.
A CyCLONe atua primariamente ao nível operacional, quando ocorre uma crise transfronteiriça no ciberespaço em larga escala. Os contactos desta Rede procuram interligar o nível técnico (Rede CSIRT-EU) com o nível político, com o objetivo de apoiar a gestão coordenada desses incidentes e crises de cibersegurança. Neste sentido, a garantia do intercâmbio regular de informações entre os Estados-Membros e as instituições, organizações e agências da UE também é uma importante meta a cumprir. Para tal, procura-se, ao nível operacional do projeto, uma cooperação eficaz entre as Organizações de Ligação para Crises no Ciberespaço (CyCLO), ou seja, as autoridades competentes dos Estados-Membros dentro da CyCLONe.
Em 19 de maio de 2021, Portugal organizou o exercício CySopex 2021 no âmbito da Presidência da UE, para testar precisamente os procedimentos dos Estados-Membros na gestão rápida de crises transnacionais em grande escala no ciberespaço[23]. É expectável que a supramencionada Diretiva SRI 2 venha — pela primeira vez — a plasmar normativos que promovam o enquadramento legal da CyCLONe.

Perante a necessidade crescente na UE de uma resposta policial ao crime organizado no ciberespaço, a EUROPOL estabeleceu, em 2013, o Centro Europeu de Cibercriminalidade (EC3), um organismo especializado no apoio operacional, elaboração de estratégias, investigação e desenvolvimento, em particular no domínio forense[24]. Ao nível operacional, centra-se principalmente no crime ciberdependente, na exploração sexual de crianças em linha e na fraude de pagamentos.

18 Sobre a ENISA ver *Relatório Ética & Direito 2020* (CNCS 2020c).

19 https://csirtsnetwork.eu.

20 A Rede Nacional CSIRT é composta por equipas de resposta rápida a incidentes de entidades públicas e privadas, na qual é dinamizado um fórum de discussão técnica. Este fórum pode emitir recomendações e promover formas de cooperação entre as CSIRT, assim como entre estas e parceiros externos, sobre matérias relativas à segurança informática. A adesão a esta rede é voluntária (https://www.redecsirt.pt).

21 Refira-se que o CERT.PT é também membro de duas outras redes de cooperação internacional: o *Forum of Incident Response Teams* (FIRST) e a *Trusted introducer for CSIRTs in Europe* (TF-CSIRT). O FIRST, criado em 1990, reúne equipas de segurança e resposta a incidentes do mundo inteiro, em especial equipas de segurança dos setores governamental, comercial e académico (https://www.first.org/). Já no âmbito do TF-CSIRT, o serviço *Trusted Introducer* foi criado na Europa em 2000 para apoiar a colaboração entre equipas de resposta a incidentes, fornecendo entre outros um Diretório pesquisável que funciona como uma base de dados com todas as equipas registadas e conhecidas dentro desta comunidade (https://www.trusted-introducer.org/index.html).

22 https://www.cyclone-project.eu/.

23 https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management.

24 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

A atuação do EC3 junto dos Estados-Membros pauta-se por oferecer apoio operacional e analítico às suas investigações criminais, além de prestar formação às suas autoridades competentes[25].

É no âmbito da Organização do Tratado do Atlântico Norte (OTAN/NATO), aliança transatlântica de defesa coletiva e segurança cooperativa que Portugal, enquanto Aliado (membro fundador), coopera na partilha de informação e assistência mútua na prevenção, mitigação e recuperação de ciberataques.
Apesar de cada Aliado ser responsável pela sua própria ciberdefesa, da mesma forma que cada um possui os seus próprios meios genéticos (carros de combate, aeronaves e navios), a NATO apoia os seus membros no reforço dessas defesas, partilhando informação em tempo real sobre ciberameaças e mantendo equipas de defesa cibernética de reação rápida que podem ser enviadas para ajudar os Aliados. A *NATO Computer Incident Response Capability* (NCIRC) é sedeada em Mons (Bélgica), e fornece um apoio permanente à defesa cibernética das próprias redes da NATO (NATO 2019).
A Aliança Atlântica investe também na educação, formação, treino e organização de importantes exercícios conjuntos de ciberdefesa, destacando-se neste contexto a Academia de Comunicações e Sistemas de Informação da NATO (*NCI Academy*) em Oeiras, escola de formação na qual são ministrados, entre outros, cursos de ciberdefesa e cibersegurança a militares e a civis que prestem serviço na NATO ou nos países que constituem a NATO[26].

Enquanto membro da Organização para a Segurança e Cooperação na Europa (OSCE), a maior organização de segurança regional do mundo, Portugal apoia ativamente os compromissos assumidos por esta Organização nas suas três dimensões: político-militar, económico-ambiental e humana. Reconhecendo a complexidade do ciberespaço e o seu potencial para aumentar tensões entre Estados, a OSCE aborda nos seus trabalhos várias ciberameaças, incluindo cibercrimes e a utilização da Internet para fins terroristas[27]. Neste campo, os Estados-Membros da OSCE desenvolvem entre si medidas de formação de confiança e segurança (*Confidence Building Measures – CBM*), tais como a troca de informações transparentes, para reduzir os riscos de conflito decorrentes das tecnologias de informação. O ponto de contacto nacional da OSCE, ao nível da cibersegurança, é o CNCS.

25 Para mais informações, consultar o *Relatório Ética & Direito 2020* (CNCS 2020c).
26 https://www.ncia.nato.int/what-we-do/nci-academy.html.
27 https://www.osce.org/secretariat/cyber-ict-security.

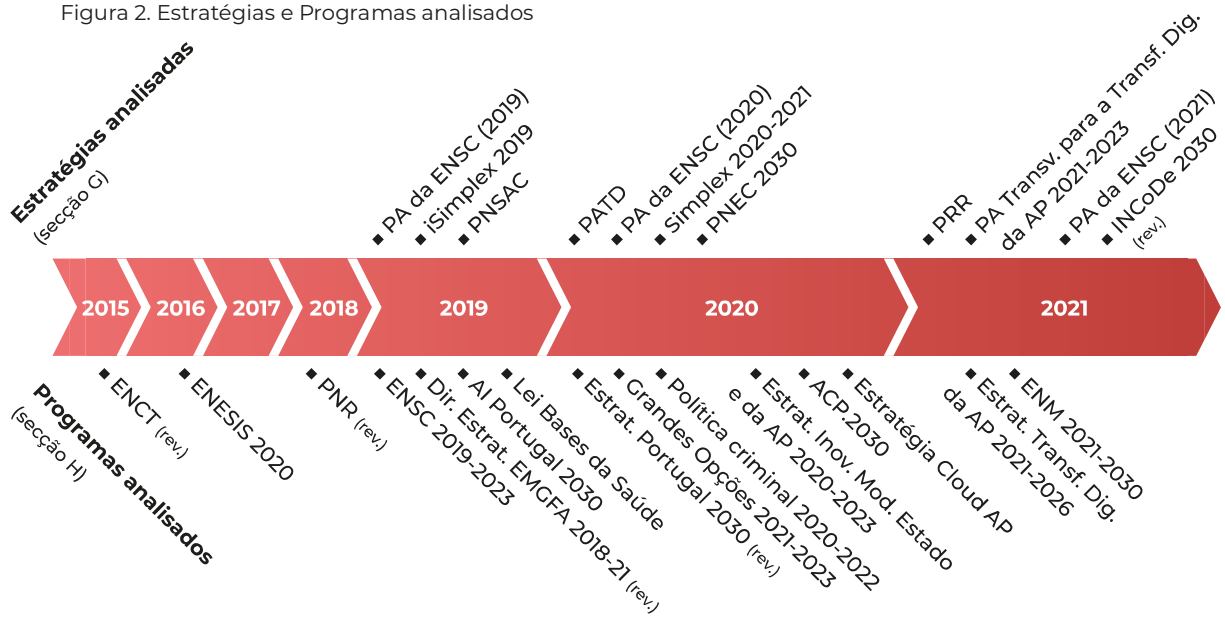
G

ESTRATÉGIAS

A conceptualização descrita na secção E enfrenta, quando aplicada ao panorama nacional, algumas dificuldades de operacionalização decorrentes de dois fatores. Por um lado, não existe uma prática de denominação dos documentos que permita efetuar uma divisão e imputação rigorosas de todos os instrumentos de política pública mapeados neste relatório à tipologia adotada. Por outro lado, vários desses documentos possuem características mistas de instrumentos estratégicos e programáticos. Neste cenário, optou-se por incluir nesta secção os instrumentos de política pública que são total ou predominantemente de natureza estratégica, relegando para a secção H (Programas Públicos) os instrumentos de cariz essencialmente operativo, ainda que alberguem orientações e diretrizes de natureza política.

A Figura 2 mostra as Estratégias e Programas Públicos nacionais analisados, organizados segundo o seu ano de aprovação (ou, quando indicado, da sua última revisão).

Figura 2. Estratégias e Programas analisados



G.1 INSTRUMENTOS ORIENTADORES DE POLÍTICA NACIONAL

Nesta subsecção são abordados os principais instrumentos que estruturam as orientações e prioridades das políticas de desenvolvimento e investimento nacionais, servindo de pilares para a elaboração de políticas públicas nacionais. No seu conjunto, estes diferentes instrumentos ilustram as grandes estratégias globais de médio prazo nas quais se sustentam as próprias Estratégias de Cibersegurança.

G.1.1 PROGRAMA NACIONAL DE REFORMAS (PNR) 2016-2022

O Programa Nacional de Reformas (PNR)[28], criado em 2016, definiu a estratégia de médio prazo do XXI Governo Constitucional para ultrapassar um conjunto de bloqueios estruturais previamente identificados. A estratégia foi revista e atualizada em 2018 (Governo Português 2018) mantendo a sua organização em seis pilares, que refletem as prioridades das políticas públicas do Governo, conforme a Figura 3.

Figura 3. Pilares do Plano Nacional de Reformas

Associado a cada um destes pilares é proposto um conjunto de reformas estruturais e de medidas de atuação. Estas podem ser consideradas isoladamente ou fazendo parte de outros instrumentos de política pública como, por exemplo, o Plano Estratégico dos Transportes e Infraestruturas (PETI) ou o Plano Ferrovia 2020. Independentemente de alguns destes instrumentos de política pública poderem tratar de questões relacionadas com a cibersegurança, no documento do PNR (versão atualizada de 2018) apenas se encontra uma breve referência direta e explícita a cibercrime referente à conclusão do projeto ComFacSYS que permitiu reforçar as capacidades tecnológicas da Polícia Judiciária.

G.1.2 ESTRATÉGIA PORTUGAL 2030

A preparação da Estratégia Portugal 2030 teve início em 2017, tendo a sua última atualização sido aprovada pela Resolução do Conselho de Ministros n.º 98/2020, de 13 novembro. Esta Estratégia serve de referência global para a estruturação dos grandes documentos de planeamento, como o Programa Nacional de Reformas e as Grandes Opções, bem como de todos os instrumentos financeiros de apoio ao desenvolvimento em Portugal até 2030.

28 https://www.portugal.gov.pt/pt/gc21/governo/programa/programa-nacional-de-reformas.aspx

A Estratégia está organizada segundo quatro agendas temáticas:

1. As Pessoas Primeiro: um melhor equilíbrio demográfico, maior inclusão, menos desigualdade;
2. Digitalização, Inovação e Qualificações como Motores do Desenvolvimento;
3. Transição Climática e Sustentabilidade dos Recursos;
4. Um País Competitivo Externamente e Coeso Internamente.

No âmbito da agenda temática dedicada à Digitalização, Inovação e Qualificações é referida a necessidade de considerar os desafios associados à cibersegurança no contexto do processo de transformação digital. Esta agenda temática está organizada segundo quatro domínios estratégicos fundamentais (Promoção da sociedade do conhecimento; Digitalização e inovação empresarial; Qualificação dos recursos humanos; Qualificação das instituições). As intervenções no domínio estratégico da Qualificação das instituições, que visam promover a modernização, capacitação e digitalização da Administração Pública e a simplificação administrativa com vista a reduzir os custos de contexto, incluem a melhoria da eficiência da Administração Pública fomentando, entre outros, o desenvolvimento de competências para o futuro, nomeadamente na áreas da cibersegurança.

G.1.3 LEI DAS GRANDES OPÇÕES (GO) PARA 2021-2023

A Lei das Grandes Opções para 2021-2023 em Matéria de Planeamento e da Programação Orçamental Plurianual (Lei das Grandes Opções – GO), foi aprovada em 31 de dezembro de 2020 e contempla o planeamento e a programação orçamental plurianual para o biénio 2021-2023 (Lei n.º 75-C/2020, de 31 de dezembro). A Lei define um conjunto de prioridades, medidas e objetivos em matéria de política económica e de políticas públicas em torno de quatro Agendas Estratégicas:

1. Pessoas, demografia, inclusão e igualdade: as pessoas primeiro, um melhor equilíbrio demográfico, maior inclusão, menos desigualdades;
2. Digitalização, inovação e qualificações como motores do desenvolvimento;
3. Transição climática e sustentabilidade dos recursos;
4. Competitividade e coesão: um país competitivo externamente e coeso internamente.

No que diz respeito a cibersegurança e questões conexas, as GO incluem as seguintes orientações relativas à valorização das funções de soberania:

- Continuar a adaptação da Defesa Nacional e a transformação das Forças Armadas para responder às novas ameaças decorrentes da utilização abusiva do ciberespaço;
- Adotar novas soluções de recrutamento, retenção e requalificação, e apostar na formação para responder às exigências da ciberdefesa;
- Monitorizar e avaliar em permanência os fenómenos de ciberataques e a cibercriminalidade.

Para esse efeito prevê-se a seguinte medida:

> Ampliar as responsabilidades e os meios do Centro Nacional de Cibersegurança, promovendo o cumprimento de uma renovada estratégia nacional para o ciberespaço.

No âmbito da Agenda "Pessoas, demografia, inclusão e igualdade" (Agenda 1) é referida ainda a necessidade de sensibilizar e capacitar os consumidores em matéria de cibersegurança.

G.2 ESTRATÉGIAS DE CIBERSEGURANÇA

Nesta subsecção são apresentadas as grandes estratégias que compõem a estrutura da cibersegurança nacional. Estas ilustram as prioridades e os diferentes palcos de atuação nos quais os principais atores da cibersegurança intervêm, nomeadamente no âmbito da cibercriminalidade, do contraterrorismo e da defesa nacional.

G.2.1 ESTRATÉGIA DE CIBERSEGURANÇA DA UE

No quadro da Estratégia da UE para a União da Segurança para o período 2020-2025, apresentada pela Comissão Europeia a 24 de julho 2020 [COM(2020) 605 final], a cibersegurança surge associada à prioridade estratégica "Ambiente de segurança a longo prazo", enquanto o cibercrime é situado na prioridade "Fazer face a ameaças em permanente evolução" (Figura 4). Não obstante, a necessidade de cibersegurança acaba por permear a estratégia de segurança na sua globalidade, sendo indissociável quer do combate ao terrorismo e crime organizado, quer da construção de um ecossistema europeu de segurança sólido.

Figura 4. Pilares da Estratégia da UE para a União da Segurança

Fonte: Comissão Europeia[29]

29 Adaptado de https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_pt#the4pillarsofthestrategy, de acordo com [COM(2020) 605 final - versão em língua portuguesa]

Neste contexto estratégico europeu, foi apresentada, em 16 de dezembro de 2020, pela Comissão Europeia e pelo Serviço Europeu de Ação Externa, a Estratégia de Cibersegurança da UE para a década digital, com o objetivo de reforçar a resiliência da Europa contra ciberataques e ciberameaças[30]. Esta Estratégia é atualmente considerada um pilar essencial de uma Europa ecológica, digital e estrategicamente autónoma. Este instrumento procura reforçar a cooperação intergovernamental em matéria de ciberdefesa, assim como fomentar a ciber-diplomacia. Subjacente à Estratégia está a necessidade crescente de uma integração mais aprofundada entre os Estados-Membros no que toca às suas capacidades e políticas que contribuam para afirmar um ciberespaço europeu seguro e resiliente ao nível coletivo[31].

A Estratégia organiza-se em torno de três eixos fundamentais:

1. Resiliência, soberania tecnológica e liderança (adoção da Diretiva SRI 2; construção de um "escudo de cibersegurança" europeu que permita a deteção precoce de ciberataques);
2. Reforço da capacidade operacional para prevenir, dissuadir e reagir (criação de uma ciberunidade conjunta envolvendo organismos da UE e autoridades nacionais responsáveis pela prevenção, dissuasão e resposta a ciberataques);
3. Promoção de um ciberespaço mundial aberto através do reforço da cooperação com os parceiros internacionais da UE (aposta na ciber-diplomacia).

Para concretizar a Estratégia, foram criados em 2021 dois órgãos específicos – a *Joint Cyber Unit* e o Centro Europeu de Competências em Cibersegurança – que se encontram atualmente em fase de implementação pela Comissão Europeia.

A nova Ciberunidade Conjunta foi apresentada pela Comissão Europeia no dia 23 de junho 2021 para responder ao aumento recente de ciberincidentes graves registados nos serviços públicos, empresas e vidas dos cidadãos da UE. A tendência que se afirma no sentido de os ciberataques serem cada vez mais importantes, tanto em dimensão como em consequências, traz a necessidade de uma cooperação ainda maior entre os Estados-Membros, assim como de uma capacidade de resposta coletiva mais avançada e coordenada que suplante o trabalho realizado separadamente pelas diferentes comunidades de cibersegurança (forças policiais, civis, diplomacia, parceiros do setor privado, etc.).
Esta Unidade propõe-se, assim, congregar recursos e conhecimentos técnicos e operacionais, mediante uma plataforma virtual e física de cooperação, na qual as instituições, organismos e agências da UE, juntamente com os Estados-Membros, convergem para formar uma rede integrada de solidariedade, assistência e resposta pronta perante os ciberataques de grande escala.
A Comissão Europeia desenhou um processo faseado para a implementação desta Ciberunidade, composto de quatro metas sucessivas para 1) avaliar os aspetos organizacionais e identificar as capacidades operacionais da UE; 2) preparar planos nacionais de resposta a crises e incidentes e organizar exercícios conjuntos de treino; 3) operacionalizar a Ciberunidade Conjunta através de equipas de reação rápida; 4) envolver parceiros do setor privado. O prazo estabelecido para a conclusão do processo e implementação plena da Ciberunidade Conjunta é 30 de junho de 2023[32].

30 https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391
31 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
32 https://ec.europa.eu/commission/presscorner/detail/pt/IP_21_3088

O Centro Europeu de Competências em Cibersegurança, localizado em Bucareste, visa estimular a investigação, inovação e a competitividade da indústria europeia no campo da cibersegurança. Trabalha juntamente com uma Rede de Centros Nacionais de Coordenação para desenvolver uma agenda comum de desenvolvimento tecnológico entre os Estados-Membros, agrupar recursos, e canalizar investimento em projetos estratégicos de cibersegurança com aplicação em áreas de interesse público (por exemplo, na área dos negócios e PME)[33]. Cada Estado-Membro nomeará assim o seu próprio Centro Nacional de Coordenação, o qual terá competências para coordenar-se com a indústria, a academia, o setor público e os cidadãos, receber subvenções diretamente da UE, e apoiar terceiros financeiramente. Neste ecossistema, as comunidades científicas e industriais, as autoridades públicas e a comunidade colaboram na partilha de conhecimentos e capacidades.
De acordo com o Regulamento de 8 de junho 2021 que estabelece o Centro e a Rede, as contribuições financeiras de cada Estado-Membro para os trabalhos destas entidades são voluntárias, funcionando em método de cofinanciamento com a UE.

G.2.2 ESTRATÉGIAS DE CIBERSEGURANÇA ADOTADAS PELOS PAÍSES DO EEE

Desde 2017, todos os países que compõem o Espaço Económico Europeu (EEE) possuem estratégias de cibersegurança (*National Cyber Security Strategies*, NCSS), cujos objetivos constam da Figura 5, de acordo com os dados publicitados pela ENISA no mapa de estratégias nacionais. A Diretiva SRI impõe a obrigação de se publicitar aquelas estratégias.

Figura 5. Objetivos das estratégias nacionais de cibersegurança

Objetivos	Austria	Bulgaria	Croatia	Denmark	Estonia	Finland	France	Germany	Hungary	Ireland	Italy	Latvia	Lithuania	Malta	Netherlands	Norway	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Switzerland
Address cyber crime	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■
Adopt Information Security Standards					■					■			■							■				
Balance security with privacy		■	■		■	■	■			■	■	■				■		■		■	■	■	■
Citizen's awareness		■		■	■	■	■	■		■	■	■	■	■		■	■	■	■	■	■	■	■
Critical Information Infrastructure Protection	■			■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■
Develop national cyber contingency plans	■			■	■	■	■	■	■	■	■	■	■			■	■		■	■		■	■
Engage in international cooperation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Establish a public-private partnership	■				■	■				■	■		■		■	■	■		■	■		■	■
Establish an incident response capability	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Establish an institutionalised form of cooperation between public agencies	■				■		■	■	■	■	■					■	■	■		■	■	■	■
Establish and implement policies and regulation capabilities										■			■							■			
Establish baseline security requirements	■		■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■		■	■
Establish incident reporting mechanisms	■	■	■	■	■	■	■		■	■	■			■		■	■	■	■	■	■	■	■
Establish trusted information-sharing mechanisms					■					■										■			
Foster R&D	■	■	■	■	■	■	■	■		■	■		■			■	■	■	■	■		■	
Organise cyber security exercises	■			■	■	■	■		■	■	■		■			■	■	■		■	■	■	■
Provide incentives for the private sector to invest in security measures						■				■	■					■				■		■	
Risk assessment approach					■					■			■							■			
Set a clear governance structure										■										■			
Strengthen training and educational programmes	■	■		■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Total	**12**	**8**	**7**	**11**	**17**	**14**	**13**	**9**	**9**	**19**	**15**	**9**	**14**	**6**	**7**	**15**	**13**	**12**	**11**	**20**	**10**	**15**	**13**

Fonte: ENISA[34]

■ Objetivo incluído na respetiva estratégia nacional

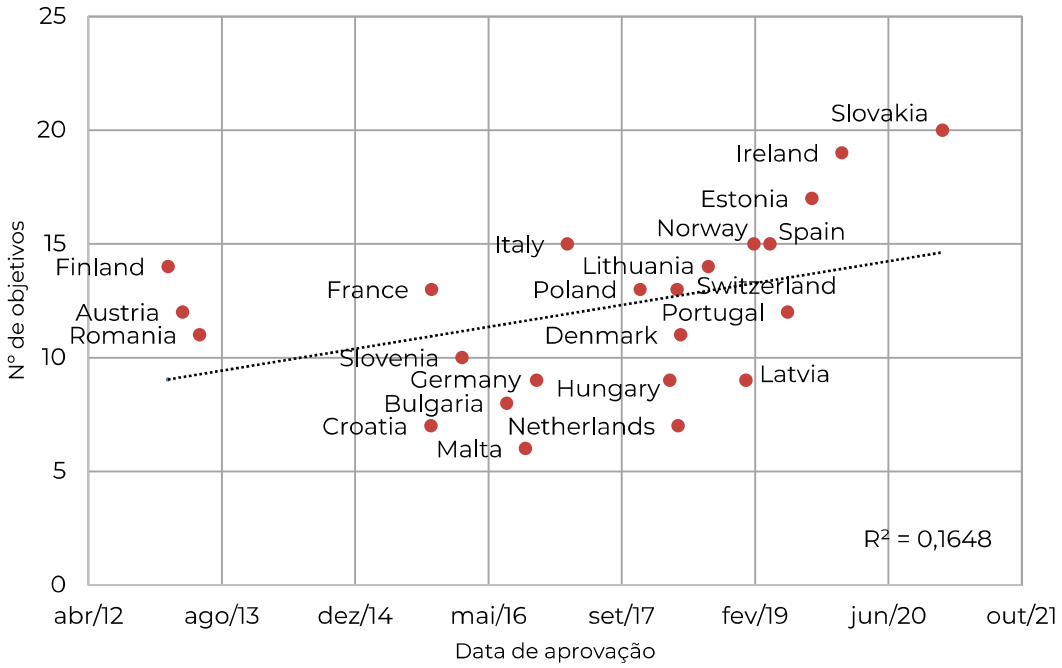
33 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre

34 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Nesta figura é patente a diversidade de objetivos propostos pelas diferentes políticas nacionais, existindo apenas dois objetivos que constam de todas as estratégias nacionais ("*Engage in international cooperation*" e "*Establish an incident response capability*").

Uma análise da evolução das estratégias ao longo do tempo (Figura 6) relaciona o número de objetivos presente em cada documento com a data da aprovação da sua versão mais recente.

Figura 6. Evolução do número de objetivos por estratégia com o tempo



Fonte: ENISA[35]

Nesta figura é possível verificar que, embora exista alguma divergência em termos de objetivos propostos por cada país (com um valor médio de 12 objetivos em 20), as estratégias mais recentes têm vindo a incorporar cada vez mais opções (como é visível na linha de tendência representada na figura. Esta linha mostra um valor médio de crescimento do número de objetivos de cerca de um objetivo por ano, com a estratégia Portuguesa a incluir um número de objetivos ligeiramente inferior à média, mesmo em relação à data da sua aprovação.

G.2.3 ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO (ENSC) 2019-2023

A ENSC 2019-2023 foi aprovada a 23 de maio de 2019 pela Resolução do Conselho de Ministros nº 92/2019, em revisão da primeira estratégia adotada em 2015. Desenvolvida para responder à constante evolução digital, a ENSC 2019-2023 apresenta uma abordagem compreensiva das necessidades de segurança do ciberespaço a nível nacional. A abordagem de segurança inerente à ENSC destina-se a proteger e defender as infraestruturas críticas, os serviços de informação, as entidades públicas e privadas, e os cidadãos, focando dimensões como a prevenção, a educação e sensibilização, o combate ao cibercrime, a investigação e o desenvolvimento, e ainda a cooperação nacional e internacional.

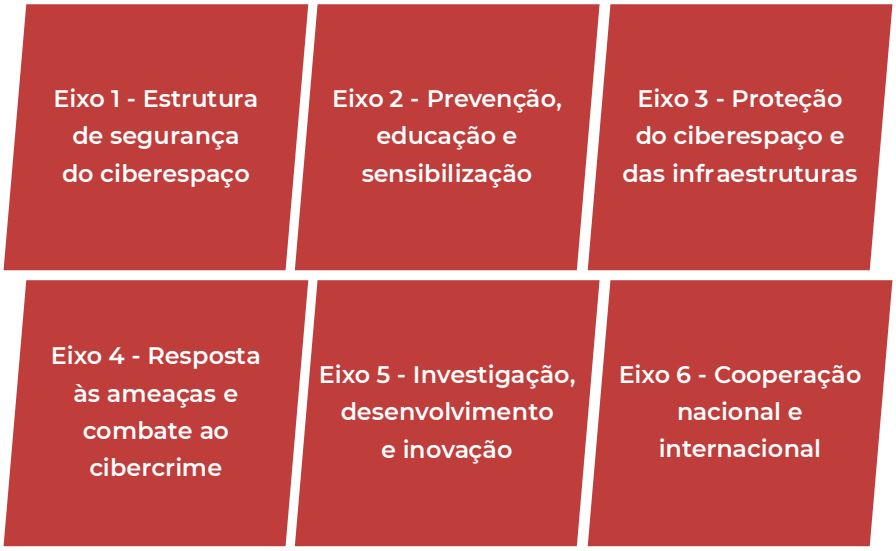
35 Elaborado a partir de informação disponibilizada em https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

A ENSC visa fazer de Portugal "um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade" (ponto 3 da ENSC).

Esta visão agregadora desenvolve-se através da prossecução de três objetivos estratégico - Maximizar a resiliência; Promover a inovação; Gerar e garantir recursos aptos à promoção da segurança do ciberespaço - os quais servem de orientação geral para os seis eixos de intervenção, que dão forma às linhas de ação concretas que visam a segurança nacional do ciberespaço.

Os seis eixos de intervenção elencados na ENSC 2019-2023 constam da Figura 7.

Figura 7. Eixos de intervenção da ENSC 2019-2023



A ENSC 2019-2023 determina a elaboração, no prazo de 120 dias após a sua aprovação, de um Plano de Ação (ver secção H.4) a rever com periodicidade anual ou sempre que necessário (CNCS 2019a, Ponto 6). Cabe ao CNCS coordenar a elaboração e acompanhar a execução e a revisão do Plano de Ação (CNCS 2019a, Ponto 3), e ao Conselho Superior de Segurança do Ciberespaço elaborar anualmente, ou sempre que necessário, um relatório de avaliação da sua execução[36].

G.2.4 DIRETIVA ESTRATÉGICA DO ESTADO-MAIOR-GENERAL DAS FORÇAS ARMADAS

O Conceito Estratégico de Defesa Nacional identifica, como se referiu, o ciberterrorismo e a cibercriminalidade como ameaças e riscos à segurança nacional e global (MDN 2013).

Ciente da revolução tecnológica em curso nas Forças Armadas, das vulnerabilidades existentes no espaço digital e do peso crescente das ciberameaças, o EMGFA incluiu na sua Diretiva Estratégica para 2018-2021 a necessidade de dinamizar a capacidade nacional de ciberdefesa como um dos nove objetivos estratégicos identificados para este período (OE2) (EMGFA 2019).

36 Cf. a alínea *d)*, do n.º 1 do art.º 6.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, transpondo para a ordem jurídica interna a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016.

O OE2 “visa dinamizar o desenvolvimento da capacidade de ciberdefesa das Forças Armadas, nos diversos elementos funcionais que constituem uma capacidade operacional – Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPII) – aprofundando a colaboração entre o Centro de Ciberdefesa e o Centro de Informações e Segurança Militares (CISMIL), os núcleos dos Ramos, o Centro Nacional de Cibersegurança, o Sistema de Informações da República (SIRP) e outros parceiros nacionais e internacionais, em particular o NATO *Computer Incident Response Capability* (NCIRC), em linha com o prescrito na Estratégia Nacional de Segurança do Ciberespaço. O efeito pretendido é dotar as Forças Armadas com capacidade acrescida para defender as redes militares contra ciberataques e realizar operações militares no ciberespaço”.

G.2.5 ESTRATÉGIA NACIONAL DE COMBATE AO TERRORISMO (ENCT)

A última revisão da ENCT foi aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro. No respeito das normas europeias e internacionais, a ENCT foca-se na identificação precoce de potenciais ameaças terroristas; na prevenção das causas que conduzem à radicalização e recrutamento de terroristas; na proteção de potenciais alvos de ataques terroristas; no desmantelamento e neutralização de iniciativas terroristas e suas redes de apoio, impedindo inclusive o acesso ao financiamento de atividades terroristas; na submissão de fenómenos terroristas à ação da justiça; no desenvolvimento de uma capacidade de resposta que limite as consequências de um eventual ato terrorista, quer ao nível humano, quer ao nível das infraestruturas.

Neste contexto, a cibersegurança é elemento indispensável na luta contra o terrorismo. É nomeadamente ao nível da proteção das infraestruturas e dos sistemas de informação críticos que a ENCT visa implementar o Plano de Ação Nacional para a Proteção contra as Ciberameaças. Ao nível operacional e judiciário, na ação de perseguir e levar fenómenos terroristas perante a Justiça, a ENCT propõe reforçar o trabalho conjunto dos diferentes intervenientes e responsáveis nas áreas da cibersegurança, ciberespionagem, ciberdefesa e ciberterrorismo, nos termos da Constituição e da Lei. Finalmente, ao nível da capacidade de resposta, a ENCT identifica também a necessidade de desenvolver mecanismos de articulação e interoperabilidade entre os diversos intervenientes na resposta pronta e eficaz ao ciberterrorismo.

A Resolução da Assembleia da República n.º 134/2017, de 28 de junho, recomenda ao Governo que elabore as estratégias e os planos de ação decorrentes da Estratégia Nacional de Combate ao Terrorismo, incluindo o Plano de Ação para a Proteção e Aumento da Resiliência das Infraestruturas Críticas e o Plano de Ação Nacional para a Proteção contra as Ciberameaças.

G.2.6 POLÍTICA CRIMINAL PARA O BIÉNIO DE 2020-2022

Os objetivos, prioridades e orientações de política criminal definidos para o biénio 2020-2022 pela Lei n.º 55/2020, de 27 de agosto, contemplam especificamente a cibercriminalidade enquanto crime de prevenção prioritária (art. 4º, alínea *d)*) e de investigação prioritária (art. 5º, alínea *e)*), o que inclui crimes cometidos por meio de um sistema informático ou de comunicação. Importa referir que esta Lei identifica a importância da cooperação, quer internacional, quer entre instituições nacionais, como elemento crítico para o sucesso das intervenções a efetuar nesta área.

G.3 ESTRATÉGIAS TRANSVERSAIS DO DIGITAL

Esta subsecção é dedicada a estratégias transversais (diferentes áreas de governação e temáticas) de transformação digital. A autonomização da análise deste conjunto de instrumentos de política pública justifica-se pelos riscos acrescidos que os processos de transformação digital comportam em matéria de cibersegurança.

G.3.1 ESTRATÉGIA PARA A INOVAÇÃO E MODERNIZAÇÃO DO ESTADO E DA ADMINISTRAÇÃO PÚBLICA 2020-2023

A Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023 foi oficialmente aprovada pela Resolução do Conselho de Ministros n.º 55/2020, de 31 de julho. A Estratégia articula-se com outros programas, planos e programas nacionais, incluindo o Plano de Ação para a Transição Digital (que contempla a digitalização do Estado como um dos três pilares), e desenvolve-se em torno de 4 eixos e 14 objetivos estratégicos (concretizados através de medidas de caráter transversal e setorial).

A Estratégia inclui uma medida explicitamente relacionada com a cibersegurança, associada ao Objetivo Estratégico 8 (Reforçar a governação global das tecnologias), incluído no Eixo 3 (Explorar a tecnologia):

> Medida 8.4 - Reforçar os níveis de cibersegurança dos organismos da Administração Pública, através do Quadro Nacional de Referência para a Cibersegurança (CNCS 2019b).

Para fazer o acompanhamento da Estratégia foi definido um conjunto de Metas, das quais faz parte uma Meta específica para a Medida 8.4:

> Meta para 2023 (Medida 8.4): 80% dos organismos TIC da Administração Pública com certificação de conformidade com o Quadro Nacional de Referência em Cibersegurança.

G.3.2 ESTRATÉGIA PARA A TRANSFORMAÇÃO DIGITAL DA ADMINISTRAÇÃO PÚBLICA 2021-2026

A Estratégia para a Transformação Digital da Administração Pública 2021-2026 (Estratégia) foi aprovada pela Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro, conforme proposta apresentada pelo grupo de projeto "Conselho para as Tecnologias de Informação e Comunicação na Administração Pública - CTIC".

A Estratégia foi elaborada em alinhamento e em coordenação com:

- a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023 (secção G.3.1 deste relatório);
- o Plano de Ação para a Transição Digital de Portugal (secção H.2 deste relatório).

Também foram considerados outros documentos, tais como:

- Estratégia Nacional para a Igualdade e a Não Discriminação 2018-2030 — Portugal + Igual;
- Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (secção G.2.3 deste relatório).

Foram ainda incorporadas na Estratégia, e no correspondente Plano de Ação, as opções definidas no Plano de Recuperação e Resiliência (secção H.1 deste relatório).

A Estratégia desenvolve-se no enquadramento dos três objetivos estratégicos do eixo «Explorar a tecnologia» da Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023 (secção G.3.1), nomeadamente:

1. reforçar a governação global das tecnologias;
2. melhorar a interoperabilidade e a integração de serviços;
3. gerir o ecossistema de dados com segurança e transparência.

A Estratégia tem como visão uma "Administração Pública mais digital: melhores serviços, maior valor" e está alicerçada em seis linhas estratégicas de atuação. A cada linha estratégica está associado um conjunto de objetivos estratégicos (40 no total das linhas estratégicas), sendo definida uma meta para cada objetivo:

1. serviços públicos digitais (7 objetivos estratégicos);
2. valorização dos dados (6 objetivos estratégicos);
3. arquiteturas de referência (8 objetivos estratégicos);
4. competências TIC (10 objetivos estratégicos);
5. infraestruturas e serviços TIC (3 objetivos estratégicos);
6. segurança e confiança (6 objetivos estratégicos).

Esta última linha estratégica justifica-se, de acordo com a Estratégia, pelo facto de a segurança e a confiança serem princípios essenciais ao desenvolvimento e prestação de serviços digitais.

Dos 6 objetivos definidos para a linha estratégica "Segurança e Confiança" destacam-se dois com relevância direta para a cibersegurança:

6.1. Promover a certificação das entidades da Administração Pública no Quadro Nacional de Referência em Cibersegurança (QNRCS). Meta: 80 % entidades TIC (ver também secção G.3.1 deste relatório).

6.2. Adesão das entidades públicas aos sistemas de suporte ao Quadro Situacional Nacional (PANORAMA – secção H.9.1 deste relatório) para a cibersegurança nacional. Meta: 2023.

Para implementar a Estratégia foi proposto um conjunto de ações transversais que compõem o respetivo Plano de Ação Transversal para a Transformação Digital da Administração Pública 2021-2023 (analisado na secção H.3).

G.3.3 ESTRATÉGIA NACIONAL DE INTELIGÊNCIA ARTIFICIAL (AI PORTUGAL) 2030

A Estratégia Nacional de Inteligência Artificial 2030[37] foi elaborada no contexto do INCoDe.2030 e reconhece a cibersegurança como uma área importante de investigação e inovação associada à Inteligência Artificial (IA). A necessidade constante de adaptação e resposta autónoma e em tempo real a novas ameaças e ataques faz da IA uma componente essencial dos algoritmos de cibersegurança (IA autónoma).

A Estratégia tem como visão posicionar Portugal como um *living lab* que permita a experimentação de novos desenvolvimentos de IA para a cibersegurança.

A Estratégia prevê ainda como ações específicas no domínio da IA para a cibersegurança a criação de *Digital Innovation Hubs* (DIH), em estreita colaboração ou integrados em DIH já existentes, bem como o reforço da colaboração de organismos nacionais com parceiros internacionais.

G.3.4 ESTRATÉGIA NACIONAL DE COMPUTAÇÃO AVANÇADA (ACP) 2030

A Estratégia Nacional de Computação Avançada 2030[38] foi elaborada no contexto do INCoDe.2030 enquanto estratégia de ciência, inovação e crescimento para promover a Computação Avançada em Portugal no contexto europeu. Abrange três grandes áreas de intervenção: criar uma infraestrutura de supercomputação; desenvolver e reter pessoas com fortes competências avançadas; e implementar uma infoestrutura de políticas públicas, de forma a promover a criação de serviços e *software* de elevado valor.

A Estratégia define nove objetivos, um dos quais (Objetivo 4) dedicado à segurança dos dados e à proteção da privacidade. No âmbito deste objetivo são identificadas as seguintes ações relacionadas com a cibersegurança:

Ação 4.1 - Elaborar um plano de cibersegurança para a Rede Nacional de Computação Avançada, em conformidade com a regulamentação Europeia;

Ação 4.2 - Implementar processos de articulação entre a Rede Nacional de Computação Avançada e o CERT RCTS (Rede Ciência, Tecnologia e Sociedade) no que diz respeito à cibersegurança;

Ação 4.3 - Implementar um mecanismo de proteção da privacidade que corresponda aos requisitos e procedimentos da indústria.

G.3.5 ESTRATÉGIA *CLOUD* PARA A ADMINISTRAÇÃO PÚBLICA

A Estratégia *Cloud* para a Administração Pública em Portugal, aprovada em novembro de 2020 (CTIC 2020), propõe um conjunto de Requisitos Técnicos Comuns para contratação de *cloud* pública que inclui, no que diz respeito ao item Proteção de dados, a necessidade de cumprir os requisitos de cibersegurança estabelecidos pela Autoridade Nacional de Cibersegurança, vigentes para projetos SAMA[39] (Arquitetura de segurança das redes e sistemas de informação (CNCS 2020a)).

37 https://www.incode2030.gov.pt/ai-portugal--2030
38 https://www.incode2030.gov.pt/computacao-avancada
39 https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/sama-2020

G.4 ESTRATÉGIAS SETORIAIS E TEMÁTICAS

Nesta subsecção são analisados instrumentos de política pública que enquadram estrategicamente as respetivas áreas de governação ou as temáticas particulares a que se dirigem. A análise visa identificar de que forma a cibersegurança e temas conexos são referidos em termos explícitos.

G.4.1 LEI DE BASES DA SAÚDE (LBS)

Aprovada pela Lei n.º 95/2019, de 4 de setembro, a LBS estabelece 37 Bases incluindo a Base 16 (Tecnologias de informação e comunicação) que, no seu ponto 1, refere explicitamente a cibersegurança nos seguintes termos:

> "O Estado deve promover a utilização eficiente das tecnologias de informação e comunicação no âmbito da saúde e da prestação de cuidados, tendo em atenção a necessidade da proteção dos dados pessoais, da informação de saúde e da cibersegurança."

G.4.2 ESTRATÉGIA NACIONAL PARA O ECOSSISTEMA DE INFORMAÇÃO DE SAÚDE (ENESIS) 2020

A Estratégia Nacional para o Ecossistema de Informação de Saúde 2020 (ENESIS 2020) foi aprovada em 2016, através da Resolução do Conselho de Ministros n.º 62/2016, de 17 de outubro, com o objetivo de responder aos desafios crescentes que se colocam ao Sistema de Informação da Saúde. Com efeito, o ecossistema de informação de saúde existente, composto por um conjunto de tecnologias, pessoas e processos, é indissociável do espaço cibernético e dos desafios e riscos associados à segurança da informação, em particular ao nível da proteção da informação dos utentes, e da segurança interna do sistema de informação dos Serviços Partilhados do Ministério da Saúde. Nesse sentido, a ENESIS 2020 identifica o "Alinhamento dos objetivos de segurança da informação e cibersegurança com os objetivos globais das entidades", assim como a "Melhoria dos instrumentos de gestão da segurança e cibersegurança através da definição de objetivos e métricas comuns" como objetivos centrais para a segurança dos processos de gestão dos sistemas de informação (SPMS 2016).

G.4.3 ESTRATÉGIA NACIONAL PARA O MAR (ENM) 2021-2030

A Estratégia Nacional para o Mar (ENM) 2021-2030 foi aprovada pela Resolução do Conselho de Ministros n.º 68/2021, de 4 de junho. Alinhada com diversos instrumentos europeus e internacionais relacionados com a proteção, preservação e sustentabilidade ecológica dos oceanos, a ENM 2021-2030 baseia-se na importância do conhecimento científico, na valorização dos ecossistemas marinhos e no seu papel como vetor de desenvolvimento sustentável.

A ENM está organizada em torno de dez grandes objetivos estratégicos (OE) para a década. A cibersegurança é associada diretamente aos objetivos estratégicos seguintes:

- OE7 — Estimular o conhecimento científico, o desenvolvimento tecnológico e a inovação azul

  Este objetivo considera fundamental apoiar o desenvolvimento e a digitalização de sistemas de observação do oceano garantido que são interoperáveis, acessíveis e seguros.

- OE9 — Incentivar a reindustrialização e a capacidade produtiva e digitalizar o oceano

  Este objetivo visa promover a digitalização das atividades associadas ao mar, garantindo a observação de boas práticas e orientações nacionais no campo da cibersegurança.

São ainda identificadas 13 áreas de aplicação dos objetivos estratégicos (áreas de intervenção prioritárias - AI), das quais se destaca a seguinte no que diz respeito à cibersegurança:

- AI9 — Portos, transportes marítimos, logística e comunicações
  Esta área é alvo de projetos de simplificação e digitalização no âmbito de medidas SIMPLEX, exigindo critérios rigorosos de cibersegurança para garantir a segurança de portos, transportes marítimos, logística, comunicações e informações.

Também o objetivo estratégico 10 (OE10 - Garantir a segurança, soberania, cooperação e governação) e a área de intervenção 13 (AI13 - Segurança, defesa e vigilância marítima) fazem referência ao facto de o setor do Mar impulsionar a ciência, a inovação e as tecnologias digitais requerendo uma atenção redobrada às questões da segurança.

Foi, entretanto, aprovado o Plano de Ação da ENM 2021-2030 (Resolução do Conselho de Ministros nº 120/2021, de 1 de setembro), do qual não consta nenhuma referência explícita à cibersegurança, embora se prevejam diversas medidas de natureza tecnológica, como, por exemplo, a medida 103 (integrada no OE7) que visa incentivar a transição digital das empresas ligadas ao mar.

H

PROGRAMAS PÚBLICOS

Para além da definição e execução de instrumentos de alto-nível, tais como as estratégias enunciadas, a prossecução de políticas públicas abrange um conjunto de programas e ações. Desde logo, o Programa do XXII Governo Constitucional 2019-2023 (Governo Português 2019) que prevê o reforço da segurança interna (ampliando as responsabilidades do CNCS e dotando-o dos meios necessários à execução da ENSC), o apoio ao investimento em competências digitais avançadas (incluindo em cibersegurança), a preparação de Portugal para a quarta revolução industrial (desenvolvendo uma infraestrutura de suporte aos desafios da cibersegurança) e a promoção de melhores práticas de cibersegurança e privacidade. Para além deste, na secção anterior (Estratégias) foi já feita referência a outros programas e ações enquadrados na respetiva estratégia, pelo que, neste ponto, far-se-á essencialmente uma análise de programas e ações identificados de forma autónoma.

H.1 PLANO DE RECUPERAÇÃO E RESILIÊNCIA (PRR)

O Plano de Recuperação e Resiliência (PRR) (Min. Planeamento 2021) é um instrumento de mitigação do impacto económico e social da crise pandémica que definiu 2020 e — pelo menos também — 2021, que surge enquadrado pelo Mecanismo de Recuperação e Resiliência, promovido pela Comissão Europeia, e foi desenvolvido a partir da visão da Estratégia Portugal 2030. Está estruturado em três grandes áreas temáticas ou dimensões estruturantes — Resiliência, Transição Climática e Transição Digital —, cada uma delas composta por diversas componentes (num total de 20), subdivididas em reformas (num total de 37) que, por sua vez, são consubstanciadas através de projetos e investimentos (num total de 83).

Das 20 componentes do PRR, há duas em que a cibersegurança tem um papel relevante, ambas associadas à dimensão Transição Digital.

A primeira corresponde à componente C16 (Empresas 4.0). Esta componente está associada a uma Reforma (Transição Digital do Tecido Empresarial) que assenta, no essencial, na revisão e atualização do Plano de Ação para a Transição Digital (secção H.2). A esta componente correspondem 3 investimentos, um dos quais (Catalisação da Transição Digital das Empresas) está estruturado através de três programas dos quais se destacam, pela sua relevância no contexto da cibersegurança, os seguintes:

A criação de *Digital Innovation Hubs* (DIH), visando a centralização de um conjunto de serviços de apoio à transição digital das empresas e facilitando o acesso a conhecimento relativo a 3 tecnologias disruptivas: IA (Inteligência Artificial), HPC (*High Performance Computing*) e Cibersegurança;

A criação de Selos de Certificações de Cibersegurança, Privacidade, Usabilidade e Sustentabilidade, incluindo a criação de plataformas de certificação, a promoção de campanhas de divulgação, e a capacitação de organismos de avaliação de conformidade.

A segunda componente é a Componente C19 (Administração Pública - Digitalização, interoperabilidade e cibersegurança), cujas reformas e investimentos se ancoram essencialmente na Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023 (secção G.3.1). A esta componente correspondem sete investimentos, dos quais se destacam:

- O reforço do quadro geral de Segurança e Cibersegurança na base da confiança para a adoção dos serviços eletrónicos, consubstanciado em quatro medidas:
  - Reforçar a capacitação em cibersegurança e segurança da informação;
  - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação;
  - Implementar o quadro nacional de cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação;
  - Criar as condições físicas e tecnológicas para a implementação e operacionalização do novo modelo de coordenação da cibersegurança e da segurança da informação.
- O reforço de financiamento em infraestruturas críticas digitais eficientes, seguras e partilhadas, incluindo financiamento para intervencionar a Rede Informática do Governo, tornando-a mais resiliente.

Ao longo do PRR surgem outras referências que podemos associar à cibersegurança:

- Na Componente 17 (Qualidade e Sustentabilidade das Finanças Públicas) está previsto um investimento nos Sistemas de Informação de Gestão Financeira Pública que abrange a implementação do SOC (*Security Operations Center*);
- Na Componente 19, o investimento em Serviços eletrónicos sustentáveis visa também incrementar a governação e capacidade de reutilização segura dos dados na AP.

O PRR estabelece um conjunto de indicadores e metas associados a estas componentes, reformas, financiamentos e projetos que constam da Tabela 1.

Tabela 1. Indicadores e metas do PRR relacionadas com a cibersegurança.

Componente	Indicador	Meta	Ano
C16	**Empresas** envolvidas em Redes de *Digital Innovation Hubs* (DIH)	4000	2025
C17	Implementação do **SOC** (*Security Operations Center*) terminada	1	2025
C19	**Novas entidades** abrangidas pelo alargamento do quadro situacional (em tempo real) da Cibersegurança Nacional	47	2027
	Organismos de avaliação de conformidade	2	2027
	Novos **auditores**	12	2027
	Sistemas e infraestruturas com certificação e acreditação de segurança	24	2026
	Entidades que adotaram o sistema SEIF [Sistema de Segurança Eletrónica da Informação]	34	2026
	Entidades públicas que adotaram a solução de Criptografia Nacional	150	2026
	Informação preservada com requisitos especiais de segurança de acordo com um novo modelo de preservação digital	80%	2026
	Processos de credenciação desmaterializados através da plataforma CRESO	90%	2026
	Serviços mais procurados acedidos de forma segura através de identidade eletrónica	25	2026
	Criação de uma **rede de centros de competência em cibersegurança**	7	2026
	Criação de uma **academia de cibersegurança**	1	2026
	Formandos abrangidos por ações de formação e programas de estágios no CNCS para trabalhadores de organismos TIC da AP	9800	2026

Fonte: PRR (Min. Planeamento 2021) ANEXO Parte 2 – Metas por Componente e Investimento

H.2 PLANO DE AÇÃO PARA A TRANSIÇÃO DIGITAL (PATD)

O Plano de Ação para a Transição Digital (PATD) foi aprovado em abril de 2020, através da Resolução do Conselho de Ministros nº 30/2020, de 21 abril, e visa promover a aceleração da transição digital em Portugal.

A elaboração do PATD assentou na análise de 21 programas e estratégias (nacionais e da Comissão Europeia, do domínio digital, da esfera pública e privada), congregando diversos programas e estratégias existentes em Portugal no âmbito da área digital, incluindo o INCoDe.2030 e o Indústria 4.0.

Da análise efetuada resultou a inclusão de 57 iniciativas/medidas, das quais se destacam 12 iniciativas prioritárias, agrupadas em três Pilares de atuação fundamentais (divididos em sub-pilares) e num conjunto de Catalisadores transversais.

No que diz respeito aos Pilares de atuação, foi identificada a seguinte Medida com referência explícita à cibersegurança:

> Medida 24 - Disseminar ferramentas de Maturidade Digital e de Cibersegurança: Medida associada ao Pilar II (Transformação digital do tecido empresarial; Sub-pilar - Tecido empresarial, com foco nas PME), constante do Programa Indústria 4.0 e a ser coordenada pelo IAPMEI, I.P..

O PATD contempla ainda um Catalizador de transição digital dedicado à cibersegurança (1 - Regulação, privacidade, cibersegurança e ciberdefesa), ao qual estão associadas as seguintes Medidas com relevância neste âmbito:

> Medida 43 - Acompanhamento do programa ENSC — Estratégia Nacional de Segurança do Ciberespaço, a ser coordenada pelo CNCS;

> Medida 44 - Gestão de risco de inovação (ações de suporte aos desafios da cibersegurança), constante do Programa Indústria 4.0 e a ser coordenada pela COTEC;

> Medida 45 - Capacitação e ajuste organizacional da estrutura nacional de DPO (Data Protection Officer), a ser coordenada pela Comissão Nacional de Proteção de Dados.

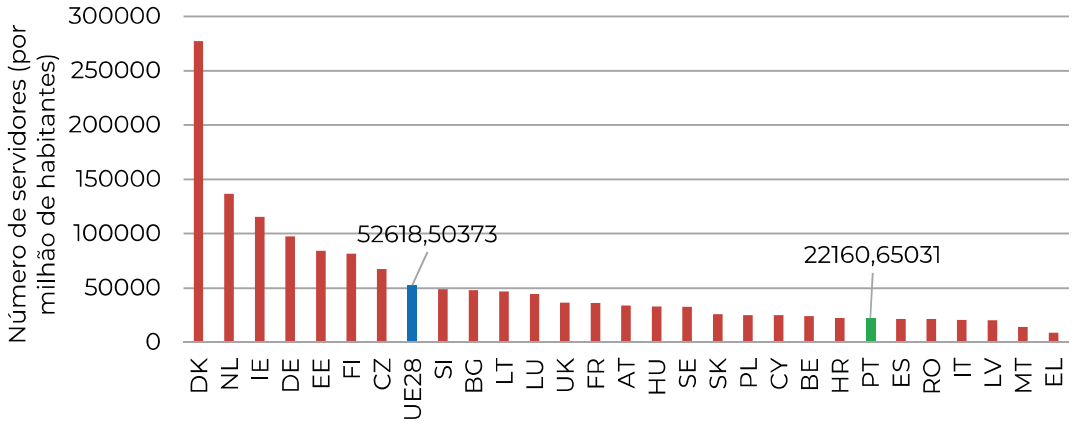
O Plano estabelece um conjunto de 97 indicadores, dos quais 48 são prioritários (que serão alvo de uma monitorização e reporte mais minucioso) e 49 complementares.

Os sete indicadores associados a estas medidas, para efeitos de monitorização de impacto do PATD, são os seguintes[40]:

40 O Relatório Riscos & Conflitos 2020 (CNCS 2020e) e o Relatório Sociedade 2020 (CNCS 2020d) apresentam análises complementares e mais detalhas de alguns dos dados que se seguem.

1. Número de servidores de Internet seguros (por milhão de habitantes) [Indicador prioritário do PATD[41]]

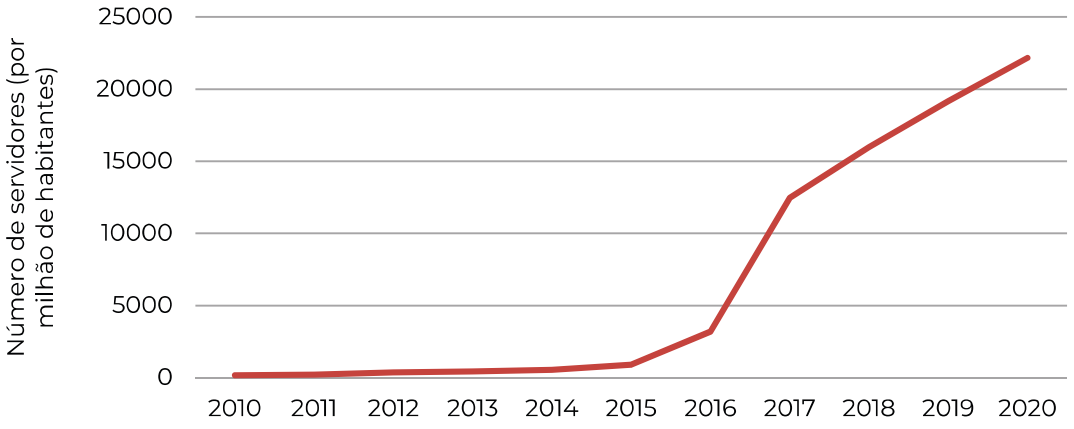
Figura 8. Número de servidores de Internet seguros (por milhão de habitantes): comparação com UE28



Fonte: (Banco Mundial 2020)

Em 2020, Portugal surge neste indicador na 22ª posição (com 22 160 servidores seguros por milhão de habitantes) de uma lista liderada pela Dinamarca (com 277 081) e abaixo da média dos 28 países da UE que é de 52 618 servidores seguros[42] por milhão de habitantes.

Figura 9. Número de servidores de Internet seguros (por milhão de habitantes): evolução de Portugal



Fonte: (Banco Mundial 2020)

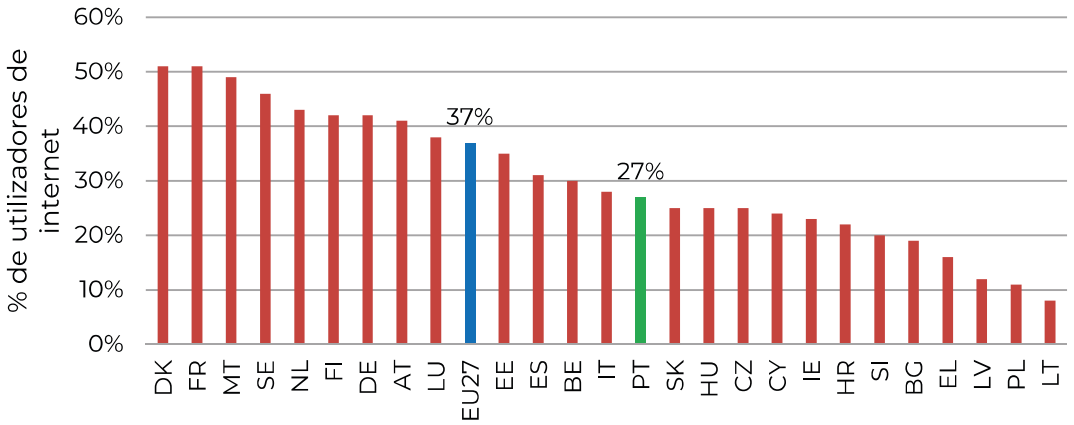
Apesar de ainda se encontrar abaixo da média europeia, Portugal tem vindo a progredir significativamente neste indicador desde 2016.

41 Embora no PATD o indicador pareça ser apresentado em número absoluto de servidores, optou-se por apresentar aqui em números relativos (por milhão de habitantes).

42 Definido como "The number of distinct, publicly-trusted TLS/SSL certificates found in the Netcraft Secure Server Survey."

2. Problemas de segurança relacionados com a utilização da Internet para fins privados [Indicador prioritário do PATD]

Figura 10. Indivíduos que experienciaram um problema de segurança com a utilização da Internet – 2019 (UE27)

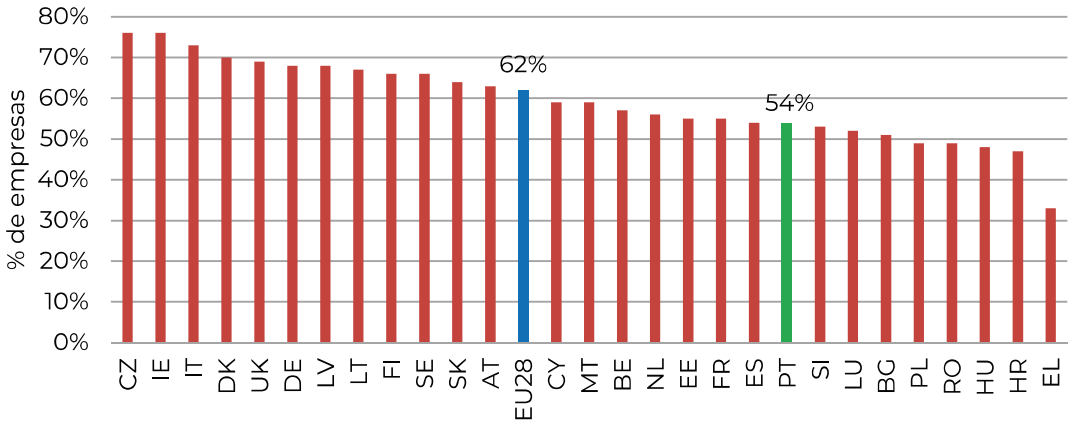


Fonte: (Eurostat 2021c). Nota: não estão disponíveis dados para a Roménia

Em 2019, e de acordo com a Figura 10, a percentagem de utilizadores de Internet que experienciaram um problema de segurança em Portugal (27%) foi inferior à média registada para os utilizadores da UE (37%).

3. Empresas tomam a iniciativa de instruir os seus colaboradores quanto às suas obrigações no respeitante à cibersegurança [Indicador complementar do PATD]

Figura 11. Empresas que sensibilizam os colaboradores sobre as suas obrigações em aspetos relacionados com a segurança das TIC – 2019 (UE28)

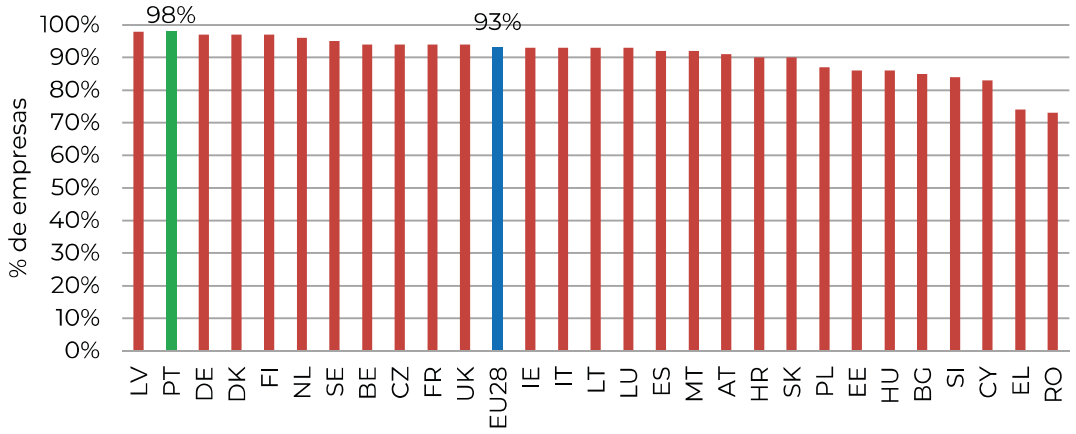


Fonte: (Eurostat 2021b)

O comportamento dos colaboradores é, no contexto empresarial, fundamental na prevenção de ocorrências e mitigação de riscos associados à utilização de TIC. No entanto, de acordo com a Figura 11, apenas 54% das empresas portuguesas (percentagem inferior à média europeia – 62%) sensibilizam os colaboradores acerca das suas obrigações em aspetos relacionados com a segurança das TIC.

4. Empresas que implementam medidas (políticas e procedimentos) de cibersegurança [Indicador complementar do PATD]

Figura 12. Empresas que implementaram uma medida de segurança de TIC – 2019 (UE28)

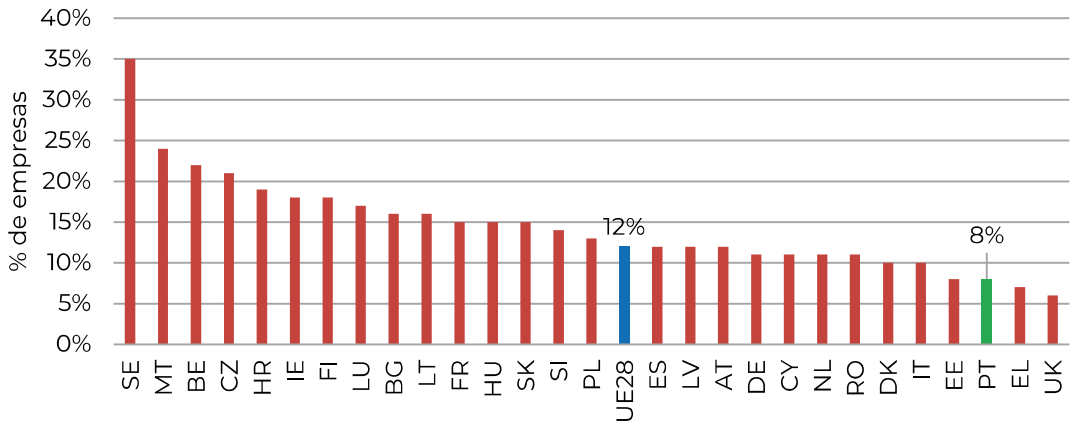


Fonte: (Eurostat 2021b)

A Figura 12 mostra que a quase totalidade (98%) das empresas em Portugal (empresas com 10 ou mais trabalhadores, exceto setor financeiro) implementou uma medida de segurança das TIC, um valor pouco superior à média europeia (93%).

5. Empresas que sofreram, pelo menos uma vez, problemas decorrentes de um incidente de cibersegurança nos seus sistemas TIC [Indicador prioritário do PATD]

Figura 13. Empresas que sofreram, pelo menos uma vez, problemas decorrentes de um incidente de cibersegurança nos seus sistemas TIC – 2019 (UE28)



Fonte: (Eurostat 2021a)

Apesar da relativamente baixa percentagem de empresas que implementa medidas de cibersegurança, a Figura 13 mostra que a percentagem de empresas portuguesas que sofreu um incidente de cibersegurança (8%) é relativamente baixa quando comparada com a média europeia (12%). Apenas dois países registaram percentagens mais baixas.

6. Organismos Públicos que utilizam alguma das seguintes medidas de segurança das TIC [Indicador prioritário do PATD]

Tabela 2. Medidas de segurança das TIC utilizadas por Organismos da AP Central, AP Regional e CM - 2020

	AP Central	AP Regional (Açores)	AP Regional (Madeira)	CM
	%	%	%	%
Atualização regular do *software*	93	100	96	99
Controlo de acessos à rede do Organismo	88	94	75	92
Autenticação dos utilizadores através de uma palavra passe segura	83	98	91	84
Conservação de registos para análise depois da ocorrência de incidentes de segurança	75	75	63	81
Avaliação dos riscos ligados às TIC	56	47	46	48
Testes de segurança às TIC	54	47	50	50
Técnicas de encriptação de dados, documentos ou e-mails	49	59	48	51
Identificação e autenticação do utilizador através de métodos biométricos	28	41	38	45

Fonte: IUTICAP 2020 (DGEEC 2021a) e IUTICCM 2020 (DGEEC 2021b)

No que diz respeito aos organismos públicos (Administração Pública Central, Regional e Câmaras Municipais), há uma grande disparidade na adoção de diferentes medidas de segurança na utilização de TIC (Tabela 2). Assim, se a quase totalidade dos organismos atualiza regularmente o seu *software* e implementa controlo de acessos à sua rede interna, o mesmo não acontece relativamente à utilização de dados biométricos para identificação e autenticação dos utilizadores dos sistemas. Outros tipos de medidas muito relevantes, como a avaliação de risco e a realização de testes de segurança, apenas são adotadas por cerca de 50% dos organismos.

7. Organismos Públicos que consciencializam o pessoal ao serviço para as suas obrigações em matéria de segurança das TIC [Indicador complementar do PATD]

Tabela 3. Tipo de ação efetuada junto do pessoal ao serviço em Organismos da AP Central, Regional e CM - 2020

	AP Central	AP Regional (Açores)	AP Regional (Madeira)	CM
	%	%	%	%
Ações de formação voluntária ou informação interna disponível	68	65	59	62
Ações de formação obrigatória e/ou consulta obrigatória de informação	26	16	27	19
Disposições contratuais	25	14	9	20

Fonte: IUTICAP 2020 (DGEEC 2021a) e IUTICCM 2020 (DGEEC 2021b)

A Tabela 3 mostra que são ainda relativamente poucos os organismos da AP Central, Regional e CM que recorrem a disposições contratuais e a ações de formação obrigatória para consciencializar os seus colaboradores relativamente às suas obrigações no âmbito da cibersegurança. O esforço de sensibilização parece assim assentar em ações de formação e acesso a informação realizado de forma voluntária. Programas do CNCS como o *Train the Trainers* (secção H.9.1) constitui um instrumento essencial para melhorar esta situação.

Embora não faça parte do conjunto de indicadores explicitamente previstos no PATD, a informação que consta da Tabela 4 permite conhecer e acompanhar as estratégias adotadas pela Administração Pública (AP Central, Regional e CM) no que diz respeito à segurança de utilização das TIC.

Tabela 4. Organismos da AP Central, Regional e CM que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC - 2020

	AP Central	AP Regional (Açores)	AP Regional (Madeira)	CM
	%	%	%	%
Organismos que possuem recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC	53	51	25	38
Assuntos considerados nessas recomendações:				
Gestão dos níveis de acesso às TIC	96	100	93	92
Armazenamento, proteção, acesso e processamento de dados	94	100	100	92
Responsabilidade, direitos e deveres no que respeita à utilização das TIC	94	92	100	91
Formação do pessoal ao serviço para uma utilização segura das TIC	91	92	100	92
Procedimentos ou regras para prevenir ou reagir a incidentes de segurança	83	77	93	85

Fonte: IUTICAP 2020 (DGEEC 2021a) e IUTICCM 2020 (DGEEC 2021b)

Estando a consciencialização dos colaboradores da AP Central, Regional e CM tão dependente da consulta voluntária de informação interna (Tabela 3), é importante que os organismos possuam e disponibilizem documentos sobre medidas, práticas ou procedimentos de cibersegurança. A Tabela 4 mostra que apenas 53% dos organismos da AP Central disponibilizam esse tipo de documento (com recomendações), baixando para 25% no caso da AP Regional (Madeira). Em geral, existindo documentação, ela cobre os principais temas relevantes. A informação e formação disponibilizadas pelo CNCS (secção H.9.1) pode dar um contributo decisivo para melhorar estes indicadores.

H.3 PLANO DE AÇÃO TRANSVERSAL PARA A TRANSFORMAÇÃO DIGITAL DA ADMINISTRAÇÃO PÚBLICA 2021-2023

O Plano de Ação Transversal para a Transformação Digital da Administração Pública (Plano de Ação Transversal) foi aprovado e publicado juntamente com a Estratégia para a Transformação Digital da Administração Pública 2021-2026 (secção G.3.2).

A versão aprovada e publicada do Plano de Ação Transversal agrega um conjunto de medidas prioritárias e ações transversais a desenvolver até ao final de 2023, enquadrando as iniciativas setoriais de transformação digital que cada área governativa levará a cabo e que serão detalhadas e disponibilizadas no site TIC.Gov.PT (As Tecnologias de Informação e Comunicação na Administração Pública)[43].

Estas medidas e ações contribuem para a implementação da Estratégia para a Transformação Digital da Administração Pública 2021-2026 (Estratégia) e distribuem-se pelas seis linhas estratégicas da seguinte forma:

- Linha Estratégica I — Serviços Públicos Digitais (2 medidas que incluem 9 ações)
- Linha Estratégica II — Valorização dos Dados (2 medidas que incluem 5 ações)
- Linha Estratégica III — Arquiteturas de Referência (2 medidas que incluem 9 ações)
- Linha Estratégica IV — Competências TIC (6 medidas que incluem 11 ações)
- Linha Estratégica V — Infraestrutura e Serviços TIC (3 medidas que incluem 4 ações)
- Linha Estratégica VI — Segurança e Confiança (4 medidas que incluem 7 ações)

Das medidas incluídas na Linha Estratégica VI (Segurança e Confiança) destacam-se duas com relevância direta para a cibersegurança. São medidas que visam atingir os objetivos definidos na Estratégia através da prossecução de um conjunto de ações específicas com datas de conclusão pré-determinadas:

Medida 6.1 — Conformidade com o Quadro Nacional de Referência para Cibersegurança (QNRCS)

- Criar o ecossistema de certificação para o QNRCS no âmbito do Quadro Nacional de Certificação em Cibersegurança (CNCS; 4º Trim 2022);
- Certificação de conformidade das entidades TIC em QNRCS (Organismos da AP; 4º Trim 2024).

Medida 6.4 — Contributo para o conhecimento situacional da cibersegurança nacional

- Adesão ao PANORAMA (CNCS; 4º Trim 2023);
- Adesão das entidades da AP ao PANORAMA (Organismos da AP; 4º Trim 2023).

43 https://tic.gov.pt

H.4 PLANO DE AÇÃO DA ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

O processo de gestão do ciclo de vida da ENSC (secção G.2.3) estabeleceu a recolha anual de atividades a inscrever no plano de ação em períodos bianuais. Essa recolha é feita diretamente junto dos organismos e serviços da Administração Pública, tendo 2020 contado também com uma iniciativa para esse efeito desenvolvida pelo Centro Nacional de Cibersegurança, que o designou por "Fórum de Cibersegurança da Administração Pública".

O Plano de Ação da ENSC (CNCS 2020b, 2021a, 2021b), na sua última revisão (2020), contempla a realização de 667 atividades programadas entre 2019 e 2021, das quais 637 atividades têm metas de caráter prospetivo para o biénio 2020/2021. O desenvolvimento destas atividades é da responsabilidade de organismos e serviços da Administração Pública (referentes a 18 áreas governativas e incluindo Regiões Autónomas), de um órgão consultivo (o Conselho Superior de Segurança do Ciberespaço), contando com o envolvimento de organizações da sociedade civil, como a APAV e a DECO. Para 2020, o Plano de Ação da ENSC incluiu atividades de 67 serviços e organismos da Administração Pública.

Embora alinhadas com os eixos de intervenção da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, as atividades inscritas no Plano de Ação da ENSC podem ser mais bem categorizadas e analisadas de acordo com a sua natureza e foco, considerando os objetivos que os organismos pretendem atingir com a sua realização, conforme a Tabela 5.

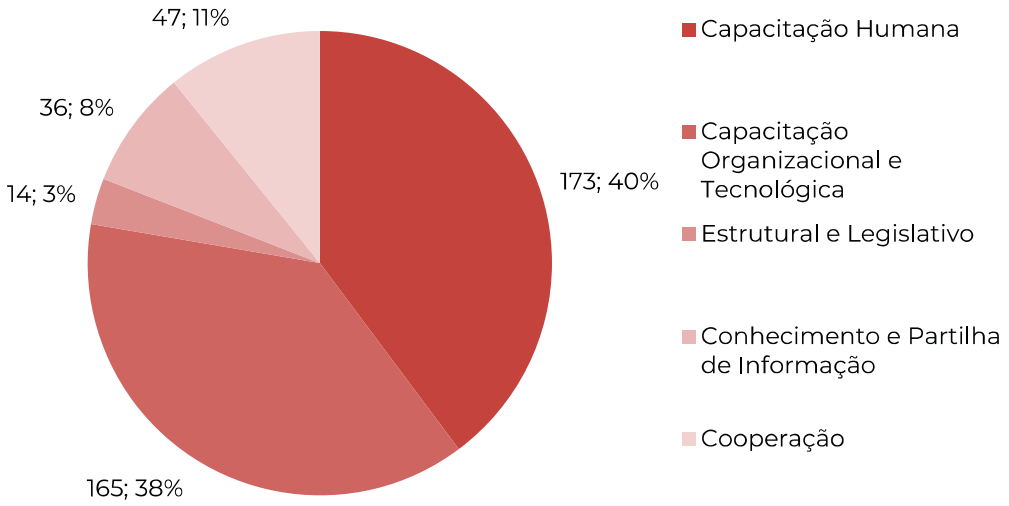
Tabela 5. Natureza e foco das atividades inscritas no Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço

Natureza	Foco
Estrutural	Decisão/Avaliação Estratégica Nacional e Regional
Capacitação Humana	Formação/Sensibilização Cidadãos
	Formação/Sensibilização Recursos Humanos
	Formação/Sensibilização Especialistas
	Formação/Sensibilização Decisores
	Conteúdos Formação/Sensibilização
	Outras Acções para a Formação/Sensibilização
Capacitação Organizacional e Tecnológica	Gestão de Cibersegurança
	Exercícios e Operações de Cibersegurança
	Identificação, Contratação e Retenção de Profissionais
Conhecimento e Partilha de Informação	Promoção do Conhecimento
	Investigação, Desenvolvimento e Inovação
	Partilha de Informação (operacional)
	Estruturas de Governação (setorial)
Cooperação	Cooperação Nacional
	Cooperação Internacional

Fonte: (CNCS 2021b)

Não sendo viável a descrição detalhada de todas as atividades inscritas no Plano de Ação da ENSC, apresenta-se na Figura 14 a distribuição das atividades desenvolvidas em 2020 categorizadas segundo a sua natureza.

Figura 14. Natureza das atividades desenvolvidas em 2020 no âmbito do Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço



Fonte: (CNCS 2021b)

Segundo a Figura 14, uma percentagem muito significativa das atividades do Plano de Ação da ENSC diz respeito à capacitação humana (173 atividades, 40% do total), organizacional e tecnológica (165 atividades, 38% do total). Algumas atividades são identificadas e descritas individualmente ao longo deste relatório, estando incluídas e/ou correlacionadas com outras estratégias, programas e planos.

H.5 INICIATIVA NACIONAL DE COMPETÊNCIAS DIGITAIS E.2030 – INCODE 2030

O programa Iniciativa Nacional Competências Digitais e.2030, Portugal INCoDe.2030, foi criado oficialmente através da Resolução do Conselho de Ministros n.º 26/2018, de 8 de março, e concretizou uma estratégia para o desenvolvimento digital do país, no âmbito do Programa Nacional de Reformas, alinhada com a iniciativa Indústria 4.0 — Estratégia Nacional para a Digitalização da Economia.

O INCoDe.2030 foi revisto e reformulado através da Resolução do Conselho de Ministros n.º 59/2021, de 14 de maio, considerando a aprovação do Plano de Ação para a Transição Digital, a aprovação da Estratégia para a Inovação do Estado e da Administração Pública 2020-2023 e a atualização da Estratégia Portugal 2030.

O INCoDe.2030 desenvolve-se através de iniciativas promovidas por entidades públicas e privadas, organizadas segundo cinco Eixos:

- Eixo 1 — Educação e formação profissional
- Eixo 2 — Qualificação e requalificação
- Eixo 3 — Inclusão
- Eixo 4 — Formação avançada
- Eixo 5 — Investigação

No âmbito do INCoDe.2030 foram já desenvolvidas as seguintes estratégias temáticas:

- Estratégia Nacional de Inteligência Artificial 2030 / *AI Portugal 2030;*
- Estratégia Nacional de Computação Avançada 2030 / *Advanced Computing Portugal 2030;*
- Estratégia Nacional de Dados Abertos.

No conjunto de iniciativas iniciais que constituem o INCoDe.2030, sem prejuízo de outras que venham a ser adicionadas posteriormente, foi identificada uma iniciativa que diz respeito diretamente ao tema da cibersegurança:

Academia de Cibersegurança[44]. Com o objetivo de reforçar a capacitação em cibersegurança e segurança da informação através da criação de um programa de formação que dotará de competências avançadas um conjunto de novos especialistas em cibersegurança e segurança da informação oriundos da Administração Pública e do setor privado. Meta para 2023: 9800 profissionais qualificados ou requalificados. Área governativa responsável: Presidência do Conselho de Ministros (através do CNCS).

Para além de metas identificadas para cada uma das iniciativas, o INCoDe.2030 define ainda um conjunto de indicadores e as metas a utilizar para a monitorização da evolução das competências digitais em Portugal, embora nenhuma diretamente associada ao tema da cibersegurança.

H.6 PROGRAMA SIMPLEX

O programa SIMPLEX[45], lançado em 2006[46], visa fomentar a simplificação administrativa e legislativa, de modo a facilitar a relação de cidadãos e empresas com os organismos da Administração Pública portuguesa e, simultaneamente, melhorar a sua eficiência interna. É um programa que se renova anualmente com a inclusão de novas medidas de simplificação. Nas suas duas últimas edições (2019 e 2020), incluiu as seguintes medidas relacionadas com a cibersegurança:

Simplex 2020/2021[47]: Medida Sandbox4all – "Disponibilizar aos cidadãos e empresas um serviço que permita a qualquer pessoa submeter para análise uma mensagem de correio eletrónico para saber se se trata de uma mensagem maliciosa". Organismo responsável: CNCS.

iSimplex 2019[48]: Medida Ciber Check-Up – "Disponibilizar um instrumento de autoavaliação através do qual as empresas possam aferir online, de forma voluntária e interativa, a maturidade das organizações, nos domínios [i] da prevenção, deteção e reação a incidentes de cibersegurança e [ii] da gestão da segurança da informação." Organismo responsável: CNCS [Concluída, ver secção H.9.2]

44 Esta iniciativa foi posteriormente incluída no PRR (secção H.1).
45 https://www.simplex.gov.pt/
46 http://historico.simplex.gov.pt/
47 https://www.simplex.gov.pt/
48 https://www.simplex.gov.pt/simplex2019/

H.7 PLANO NACIONAL ENERGIA E CLIMA (PNEC) 2030

O Plano Nacional Energia e Clima 2030 (PNEC 2030), aprovado pela Resolução do Conselho de Ministros n.º 53/2020, de 10 de julho, constitui o principal instrumento de política energética e climática nacional para atingir um futuro neutro em carbono.

A visão estabelecida para o PNEC 2030 assenta em oito objetivos (associados a metas que Portugal pretende alcançar), para os quais foram definidas 58 linhas de atuação (objetivos políticos associados aos eixos/objetivos nacionais assumidos para o horizonte 2030) e 206 medidas de ação (ações concretas que contribuem diretamente para alcançar as metas e objetivos).

No contexto da Linha de Atuação 4.4 (Promover a Digitalização do Sistema Energético), está prevista a Medida de Ação 4.4.2 [Promover o desenvolvimento das redes inteligentes (*smart grids*)], que visa fomentar a inovação no planeamento das redes de transporte e distribuição, considerando a necessidade de resiliência dos sistemas e das redes, incluindo a salvaguarda da informação e segurança das redes devido a fenómenos e eventos relacionados com cibersegurança. Esta Medida de Ação tem previsto o período 2020-2030 para a sua execução.

H.8 PROGRAMA NACIONAL DE SEGURANÇA DA AVIAÇÃO CIVIL (PNSAC)

O Programa Nacional de Segurança da Aviação Civil, cuja última revisão foi aprovada pelo Decreto-Lei n.º 142/2019, de 19 de setembro, consagra o sistema nacional de segurança da aviação civil e identifica a cibersegurança como área relevante para a segurança do setor da aviação. O Programa estabelece que a regulamentação a emitir será da responsabilidade do Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, em articulação com a Autoridade Nacional da Aviação Civil (ANAC), enquanto entidade reguladora setorial.

H.9 OUTRAS INICIATIVAS DE POLÍTICA PÚBLICA DE CIBERSEGURANÇA

Nesta secção serão apresentados alguns exemplos de iniciativas e ações que, podendo ou não fazer parte de um programa público único e estruturado como tal, contribuem de forma relevante para a prossecução dos objetivos de política pública de cibersegurança.

H.9.1 ANÁLISE E DISPONIBILIZAÇÃO DE INFORMAÇÃO

A formulação de políticas públicas de cibersegurança, numa perspetiva de médio/longo prazo, e a atuação preventiva e de resposta a incidentes e ameaças, de preferência em tempo real, estão dependentes do acompanhamento do quadro situacional. As duas iniciativas descritas a seguir visam fazer esse acompanhamento, analisar os dados recolhidos e disponibilizar a informação que daí resulta.

Observatório de Cibersegurança

O Observatório de Cibersegurança[49] é uma iniciativa do CNCS que visa acompanhar a evolução do fenómeno da cibersegurança em Portugal, recolhendo, sistematizando, analisando e disponibilizando informação essencial à formulação de políticas públicas. É constituído por uma equipa multidisciplinar que aborda o fenómeno da cibersegurança segundo seis linhas de orientação: Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras. Este relatório é direcionado para a linha de orientação "Políticas Públicas".

Panorama

O serviço Panorama[50] do CNCS destina-se a operadores de serviços essenciais, de infraestruturas críticas e organismos TIC da Administração Pública aos quais são disponibilizados *dashboards* (painéis de controlo) e relatórios que refletem, em tempo real, o estado da segurança do ciberespaço de interesse nacional. Para esse efeito, o serviço recebe e correlaciona informação recebida de diversas fontes nacionais e internacionais, permitindo ao CNCS emitir alertas precoces direcionados, e tornando mais eficaz a coordenação da resposta a incidentes. Está previsto o reforço da adesão dos organismos da AP ao Panorama no âmbito da Estratégia para a Transformação Digital da Administração Pública 2021-2026 (secção G.3.2) e do Plano de Ação Transversal para a Transformação Digital da Administração Pública 2021-2023 (secção H.3).

H.9.2 DIAGNÓSTICO E REDUÇÃO DE RISCO

Para organizações e cidadãos não diretamente envolvidos em temáticas de cibersegurança é importante dispor de quadros de referência e ferramentas de diagnóstico que ajudem a identificar e colmatar lacunas que minimizem o risco de ciberincidentes. Alguns desses quadros de referência e ferramentas de diagnóstico são apresentados de seguida.

Quadro de Referência, Quadro de Avaliação, Roteiro para as Capacidades Mínimas, e CiberCheckUp

O CNCS desenvolveu e disponibiliza um conjunto de referenciais de diagnóstico, capacitação e redução de risco dirigido às organizações nacionais, com enfoque nas PME.

- O *Quadro Nacional de Referência para a Cibersegurança (QNRCS)*[51] oferece recomendações para que as organizações possam definir uma estratégia de redução do risco, implementando medidas de Identificação, Proteção, Deteção, Resposta e Recuperação contra ciberameaças;
- O *Quadro de Avaliação de Capacidades Mínimas em Cibersegurança*[52] define, para cada uma das medidas que compõem o QNRCS, três níveis de capacidade (Inicial, Intermédio e Avançado) para que as organizações consigam cumprir os cinco objetivos de Cibersegurança (identificar, proteger, detetar, responder e recuperar);

49 https://www.cncs.gov.pt/pt/observatorio/
50 https://www.cncs.gov.pt/pt/panorama/
51 https://www.cncs.gov.pt/pt/quadro-nacional/#quadro
52 https://www.cncs.gov.pt/pt/quadro-nacional/#quadro

- O *Roteiro para as Capacidades Mínimas de Cibersegurança*[53] apresenta um conjunto de ações a implementar em cada organização, enquadradas no QNRCS, de forma a criar uma capacidade mínima em cibersegurança num processo gradual dividido em cinco fases;
- *O CiberCheckUp*[54] é um instrumento disponibilizado pelo CNCS que permite aferir o estado de uma organização em termos de cibersegurança, considerando o Quadro Nacional de Referência para a Cibersegurança e o Quadro de Avaliação de Capacidades Mínimas em Cibersegurança.

Webcheck.PT

A iniciativa *Webcheck.PT*[55] é promovida pelo CNCS e pela Associação DNS.PT (.PT). Tem como principal objetivo incentivar a adoção de boas práticas que garantam a segurança, integridade e confidencialidade nas comunicações através da Internet.

No âmbito desta iniciativa é disponibilizada uma ferramenta que permite a análise de um domínio de Internet e de correio eletrónico e a verificação do nível de conformidade com os *standards* mais recentes para a comunicação segura. O diagnóstico permite a identificação das medidas técnicas necessárias para assegurar uma maior resiliência e segurança da presença e comunicação *online*.

H.9.3 SENSIBILIZAÇÃO, CAPACITAÇÃO E FORMAÇÃO

Sensibilizar organizações e cidadãos para a importância de adotar comportamentos preventivos, assim como a sua capacitação e formação, são aspetos importantes de qualquer política de cibersegurança. Algumas das iniciativas e projetos mais relevantes neste contexto serão descritos de seguida.

Exercício Nacional de Cibersegurança

O Exercício Nacional Cibersegurança (ExNCS)[56] é um exercício organizado e promovido pelo CNCS que envolve vários intervenientes e responsáveis nacionais na área da cibersegurança. Durante o exercício os intervenientes são colocados perante uma simulação de ciberataque ou incidente de cibersegurança, associado a um tema com relevância atual, visando:

- Desenvolver as capacidades de prevenção, monitorização, deteção, reação, análise e correção de incidentes por parte de entidades da área da cibersegurança;
- Promover o treino e a qualificação dos seus colaboradores;
- Promover a articulação e a cooperação entre essas entidades e colaboradores.

Em última análise, a realização destes exercícios tem como objetivo fomentar a formação, à escala nacional, de uma comunidade de conhecimento e de uma cultura de cibersegurança.

53 https://www.cncs.gov.pt/pt/roteiro-capacidades-minimas-ciberseguranaa/
54 https://www.cncs.gov.pt/pt/quadro-nacional/#cibercheckup
55 https://www.cncs.gov.pt/pt/webcheck/
56 https://www.cncs.gov.pt/pt/exercicio-nacional-ciberseguranca/

Iniciativa "Cyber Security Challenge PT" e competição "Capture The Flag" (CTF)

A iniciativa "*Cyber Security Challenge PT*"[57] visa identificar jovens talentos nacionais e atraí-los para carreiras profissionais na área de cibersegurança, no contexto mais abrangente do reforço da literacia digital e das competências digitais promovidos pelo programa INCoDe.2030 (ver secção H.5.). A competição "*Capture The Flag*", realizada anualmente no âmbito da "*Cyber Security Challenge PT*", contribui para esse objetivo desafiando equipas de estudantes a resolver desafios complexos de cibersegurança, testando as suas competências neste domínio, e reforçando a colaboração e o trabalho em rede. Esta competição visa também selecionar os representantes portugueses em provas internacionais, incluindo o "*European Cyber Security Challenge*" promovido pela ENISA, tendo a equipa de estudantes portugueses alcançado o 7º lugar nesta prova em 2021[58].

Projeto Europeu Centro Internet Segura

O Projeto Europeu Centro Internet Segura[59] é constituído por um consórcio formado pela Direção-Geral da Educação (DGE), Instituto Português do Desporto e Juventude (IPDJ), Fundação para a Ciência e a Tecnologia (FCT), Fundação Altice, Associação Portuguesa de Apoio à Vítima (APAV) e Microsoft Portugal, sendo coordenado pelo Centro Nacional de Cibersegurança (CNCS).

O projeto abrange diversas iniciativas das quais se destacam:

- o centro de sensibilização dirigido a toda a população – *Centro Internet Segura* – da responsabilidade do CNCS;
- um centro de sensibilização dirigido à comunidade escolar – *SeguraNet*[60] – da responsabilidade da DGE;
- um serviço de apoio e esclarecimento à população sobre a utilização segura da Internet e que inclui uma plataforma de denúncia de conteúdos ilegais *online – Linha Internet Segura (LIS)*[61] – operacionalizada pela APAV.

O projeto *SeguraNet* tem como missão promover, na comunidade educativa, a navegação segura, crítica e esclarecida na Internet e nos dispositivos móveis. A sua ação passa pela formação de professores, pela disponibilização de conteúdos e de recursos educativos digitais, pela dinamização de sessões de sensibilização, e pela promoção das iniciativas Desafios SeguraNet, Líderes Digitais e Semana da Internet Mais Segura.

57 https://www.cncs.gov.pt/pt/capture-the-flag/
58 https://dyn.cncs.gov.pt/pt/detalhe/art/135588/equipa-portuguesa-alcanca-7-lugar-no-european-cybersecurity-challenge-2021
59 https://www.Internetsegura.pt/
60 https://www.seguranet.pt/
61 https://www.Internetsegura.pt/lis/sobre-a-lis

Cursos de cibersegurança

Ainda no âmbito da prevenção, educação e formação, o CNCS preparou e disponibiliza, em colaboração com outras entidades, um conjunto de cursos gratuitos oferecidos em regime de *e-learning*, os quais são brevemente descritos na Tabela 6.

Tabela 6. Cursos *e-learning* desenvolvidos pelo CNCS (em colaboração com outras entidades)

Cidadão Ciberseguro[62] Curso de 3 horas, organizado em três módulos (casa, trabalho e exterior), que visa promover comportamentos mais seguros e contribuir para proteger os cidadãos de incidentes de cibersegurança.
Cidadão Ciberinformado[63] Curso de 4 horas que visa ajudar os cidadãos a verificar a veracidade da informação, nomeadamente de notícias *online*.
Cidadão Cibersocial[64] Curso de 3 horas, criado no âmbito do Centro Internet Segura, dirigido a jovens a partir dos 14 anos que visa promover uma utilização mais segura das redes sociais.
Consumidor Ciberseguro[65] Curso de 4 horas dirigido a todos os cidadãos que pretendam realizar compras *online* em segurança, alertando para os riscos envolvidos, ajudando a identificar se um determinado *site* é seguro ou qual o meio de pagamento adequado a cada situação.

A Tabela 7 apresenta outros cursos e programas de formação de caráter mais especializado oferecidos pelo CNCS, em colaboração com outras entidades.

Tabela 7. Outros cursos, de caráter mais especializado, desenvolvidos pelo CNCS (em colaboração com outras entidades)

Programa *Train the Trainers*[66] O Programa *Train the Trainers* visa a formação de colaboradores e dirigentes, de entidades parceiras do CNCS, que lidem diariamente com TIC. Uma vez completado o programa, os formandos passam a pertencer à Bolsa de Formadores CNCS e ficam aptos a desenvolver formação na sua organização e para outros públicos e organizações nacionais.
Curso Geral de Ciberhigiene[67] Este curso de 2 horas é composto por dois módulos, "Ciber(in)segurança" e "Ciber-higiene e Boas Práticas de Cibersegurança", e é dirigido a adultos interessados na temática da cibersegurança, independentemente do seu grau de conhecimento sobre o tema. Aborda potenciais riscos no uso da Internet e boas práticas para os evitar.
Curso Geral de Cibersegurança [68] Este curso destina-se a todos os adultos, independentemente dos seus conhecimentos, e visa contribuir para a sensibilização, educação e literacia em todas as questões que caracterizam o estado-da-arte da cibersegurança e do ciberespaço.

62 https://www.cncs.gov.pt/pt/curso-cidadao-ciberseguro/
63 https://www.cncs.gov.pt/pt/curso-cidadao-ciberinformado/
64 https://www.cncs.gov.pt/pt/cidadao-cibersocial
65 https://www.cncs.gov.pt/pt/curso-consumidor-ciberseguro/
66 https://www.cncs.gov.pt/pt/train-the-trainer/
67 https://www.cncs.gov.pt/pt/curso-geral-ciberhigiene/
68 https://www.cncs.gov.pt/pt/curso-geral-cibersegurança/

H.9.4 INVESTIGAÇÃO, DESENVOLVIMENTO E INOVAÇÃO

Para manter atualizado o conhecimento necessário à cibersegurança são necessários esforços contínuos de investigação, desenvolvimento e inovação, garantindo depois que os resultados são incorporados em novos produtos e serviços. A criação de *Innovation Hubs* constituem por isso um objetivo das políticas públicas dedicadas à cibersegurança.

C-Hub: Cybersecurity Digital Innovation Hub

O Despacho n.º 6269/2021, de 25 de junho, do Ministro de Estado, da Economia e da Transição Digital, procedeu ao reconhecimento do C-Hub (*Cybersecurity Digital Innovation Hub*) enquanto Pólo de Inovação Digital, para efeito da sua integração na respetiva Rede Nacional e da sua indicação para acesso à rede Europeia de EDIH (*European Digital Innovation Hubs*). A proposta de criação do C-Hub foi liderada pelo CNCS, com o apoio da Agência para a Modernização Administrativa (AMA), dando cumprimento a uma medida inscrita no Plano de Recuperação e Resiliência (secção H.1) e no Plano de Ação para a Transição Digital (secção H.2).

Cyber Academia and Innovation Hub

A *Cyber Academia and Innovation Hub* (CAIH)[69] é uma estrutura criada no Ministério da Defesa Nacional que tem como objetivo promover o conhecimento e as competências necessárias à nova geração de profissionais e apoiar o desenvolvimento de capacidades no domínio do ciberespaço. Articula a sua atividade com a Base Tecnológica e Industrial de Defesa (BTID) e o Sistema Científico e Tecnológico Nacional (SCTN). A CAIH está em fase inicial de atividade, tendo sido criado, a 5 de março de 2021, o Grupo de Trabalho para a sua implementação, constituído por especialistas com competências na área do ciberespaço.

A CAIH insere-se simultaneamente no espaço da cibersegurança e da ciberdefesa, com uma dimensão nacional que concorre para a ENSC e um nível de atuação internacional alinhado com a política de ciberdefesa da NATO, bem como com as estratégias de cibersegurança da UE.

H.9.5 OFERTA LETIVA EM INSTITUIÇÕES DE ENSINO SUPERIOR

Considerando a escassez de profissionais na área da cibersegurança, o aumento da oferta letiva de cursos superiores neste domínio é uma preocupação central das políticas públicas.

A ENISA mantém e disponibiliza uma base de dados sobre os cursos de cibersegurança oferecidos por Instituições de Ensino Superior a nível europeu. A CYBERHEAD (*Cybersecurity Higher Education Database*)[70] é constituída por registos submetidos diretamente por instituições académicas de países da UE, EFTA e outros países europeus num regime de *crowdsourcing*[71].

Em julho de 2021, a CYBERHEAD registava um total de 132 cursos (programmes) oferecidos por 25 países, incluindo sete cursos oferecidos por instituições académicas portuguesas. Dado o caráter voluntário do registo de cursos na CYBERHEAD, estes números não refletem necessariamente a totalidade da oferta de formação superior em cibersegurança em Portugal.

69 https://www.defesa.gov.pt/pt/pdefesa/CAIH
70 https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
71 https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/faq

De acordo com dados disponibilizados pela Direção-Geral de Estatísticas da Educação e Ciência (DGEEC), tratados no *Relatório Sociedade 2020* (CNCS 2020d), em 2020 a oferta de cursos superiores e não-superiores na área da cibersegurança em Portugal é a que consta da Tabela 8. No ano letivo de 2019/2020 estavam inscritos nestes cursos 636 alunos. No mesmo período foram registados 75 diplomados.[72]

Tabela 8. Cursos superiores e não-superiores na área da cibersegurança em Portugal

Tipo/Grau	Nº de cursos
Curso de Especialização Tecnológica	4
Curso Técnico Superior Profissional	6
Licenciatura	1
Mestrado	8
Doutoramento	1

Fonte: *Relatório Sociedade 2020* (CNCS 2020d)

H.9.6 COOPERAÇÃO INTERNACIONAL

Na secção F.4 foi já abordado o quadro institucional relativo à cooperação internacional. Descrevem-se aqui duas iniciativas que resultam desse quadro de cooperação.

CWIX 2021

Em junho de 2021, vinte militares do Estado-Maior-General das Forças Armadas, da Marinha, do Exército e da Força Aérea participaram no exercício"*Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX 2021)*", o maior evento de interoperabilidade de sistemas e de tecnologia da NATO[73]. A participação nacional focou-se nomeadamente nas áreas de Ciberdefesa, Comunicações e nos Sistemas de Informação Nucleares. Foram testados sistemas e soluções de interoperabilidade, e treinados os militares na preparação das redes de missão das Forças Armadas Portuguesas, para que os sistemas possam interligar-se de forma rápida e segura com os sistemas dos outros países e parceiros da NATO.

Projeto "No more ransom"

O projeto "*No More Ransom*"[74] foi lançado em julho de 2016 por quatro Parceiros Fundadores: EUROPOL (EC3- Centro de Combate ao Cibercrime); Politie, Kaspersky e McAffee. Reúne agências de polícia e empresas de segurança informática que se uniram para interromper as atividades criminosas ligadas ao *ransomware*, permitindo às vítimas recuperar os seus ficheiros sem pagarem os resgates exigidos. São parceiros nacionais do projeto o CNCS, a PJ e a Universidade do Porto.

72 Esta questão será objeto de análise e de um relatório dedicado a promover pelo Observatório de Cibersegurança do CNCS.

73 Segundo publicação de 8 de julho 2021 na página oficial do Facebook das Forças Armadas Portuguesas.

74 https://www.nomoreransom.org/pt/about-the-project.html

PERCEÇÕES

O objetivo desta secção é apresentar um quadro de indicadores que permita representar, de forma integrada, alguns aspetos da perceção pública (nacional e europeia) em domínios importantes da cibersegurança sob alçada (direta ou indireta) de políticas públicas. Pretende-se ainda aferir em que medida esses indicadores permitem confirmar as perceções (nos vários domínios), confrontando-os com outros indicadores, mais objetivos, também na área da cibersegurança, mas agora na perspetiva dos riscos efetivos, incidentes e falhas de segurança comprovados, etc. relativos à utilização de computadores pessoais, redes e sistemas *online* de acesso partilhado.

I.1 RECOLHA E ANÁLISE DA INFORMAÇÃO EM DOMÍNIO PÚBLICO EM CONTEXTO DE CIBERSEGURANÇA

A análise do conjunto de perceções sobre um problema ligado a cibersegurança deve ter em conta, obrigatoriamente:

- o volume, gravidade e impacto das ocorrências desse problema no universo sondado (região, país, zona económica, etc.);
- o contacto e a familiaridade dos utilizadores com o problema, e a formação e/ou informação que possuem sobre os assuntos afins (efeitos, atitudes preventivas/corretivas, ...) que lhes permitirá, por exemplo, identificar uma melhor resposta na presença de uma ameaça concreta no ciberespaço, ou discernir entre o rigor de *sites* fidedignos e *e-mails* legítimos, e campanhas de desinformação como a disseminação de *fake news* ou *e-mails* fraudulentos;
- o nível de confiança que os utilizadores têm nas diversas entidades responsáveis pela regulamentação associada, monitorização e combate às diferentes práticas criminais (incluindo as diferentes tipologias de crime informático) e a correlação destes dados com perceções relativas à avaliação que os cidadãos fazem da ação do Estado nos mesmos domínios.

Deve também ser colocada a questão, mais relevante ainda nos domínios das tecnologias da informação do que em outros, sobre se os problemas e/ou perceções não estarão a ser exacerbados com o intuito de "vender/valorizar" as soluções. São cada vez mais frequentes rumores sobre plataformas que se tornam obsoletas "cedo de mais" para serem substituídas, falsas ameaças para aquisição de novas aplicações/utilitários ou mudança de sistemas, piratas informáticos que são contratados para polícias do ciberespaço[75].

O teor/quantificação de qualquer perceção é, em última análise, um dado objetivo, mas que deve ser entendido na sua plenitude e em todas as suas condicionantes. Já o levantamento de dados relativos a acidentes, incidentes, ameaças, riscos, impactos económicos, etc., constituirá informação de mensuração tecnicamente mais objetiva, apesar de, também aqui, a precisão poder ser afetada por aspetos de difícil determinação. Por exemplo, o número de tentativas de fraude poderá ser contabilizado com precisão em determinados contextos, mas o número de tentativas bem-sucedidas e os prejuízos efetivos causados - pagamentos por resgate de dados, perdas reais de informação sensível ou valiosa, etc. - podem não ser comunicados/assumidos para proteger a imagem de fiabilidade de organizações. Conhecendo as eventuais limitações condicionantes da análise, o cruzamento de perceções com observáveis (mais) objetivos parece-nos, assim, um contributo importante para a consideração adequada da opinião pública em estudos conducentes, quer à formulação de novas políticas públicas nesta área concreta da cibersegurança, quer à monitorização de políticas existentes. No aspeto concreto da monitorização, adicionalmente há ainda que avaliar até que ponto as perceções "futuras" não estarão/virão a ser condicionadas mais pela deficiente comunicação das políticas e seus resultados do que pelo sucesso concreto na mitigação dos problemas que lhes deram origem. O nível real e global de vulnerabilidade no ciberespaço de um determinado país pode estar a descer consistentemente, fruto de políticas públicas bem-sucedidas na área e, no entanto, o nível de segurança percecionado pelos respetivos utilizadores pode estar também a descer, aparentemente de forma injustificada, por diferentes motivos.

Parece, por isso, particularmente relevante explorar, no contexto específico da cibersegurança, as diferentes condicionantes da perceção pública, explorando igualmente o que verdadeiramente condiciona as políticas que têm sido elaboradas. Para a maioria destas análises não estão disponíveis conjuntos de indicadores adequados, no domínio das perceções, que permitam obter conclusões seguras e recomendações fiáveis para quem legisla.

Focado no cruzamento entre perceções e políticas públicas no domínio da cibersegurança, esta secção analisa um conjunto de indicadores que podemos agrupar em três dimensões:

1. preocupação, confiança e avaliação de desempenho, relativamente às autoridades públicas *per se*, e ao seu papel na segurança do ciberespaço;
2. perceção pública sobre a resposta a ameaças;
3. avaliação do impacto das *fake news* (dada a sua importância crescente no domínio da cibersegurança).

Com estes indicadores é representada a situação portuguesa relativamente a cada um destes três tópicos e analisada a evolução temporal ocorrida, sempre que possível, apresentando o contexto nacional em correlação com o europeu. Também, e sempre que possível, os indicadores são desagregados por diferentes estratificações da população (sexo, residência, instrução, ...) para fundamentar a seleção de tipologias de destinatários, canais e modos de comunicação, por exemplo, em campanhas de formação ou outro tipo de intervenções.

75 Estando frequentemente na origem do processo a deteção/divulgação/exploração de falhas de segurança em sistemas sensíveis.

I.2 PERCEÇÕES SOBRE AUTORIDADES PÚBLICAS

Nesta secção procura-se:

- caracterizar os níveis de confiança dos portugueses nas diferentes entidades públicas nacionais e internacionais com responsabilidades legislativas, executivas e fiscalizadoras em domínios como o da cibersegurança;
- descrever as perceções dos portugueses sobre o desempenho das autoridades públicas no combate ao cibercrime;
- caracterizar a preocupação dos portugueses com a segurança dos seus dados *online*.

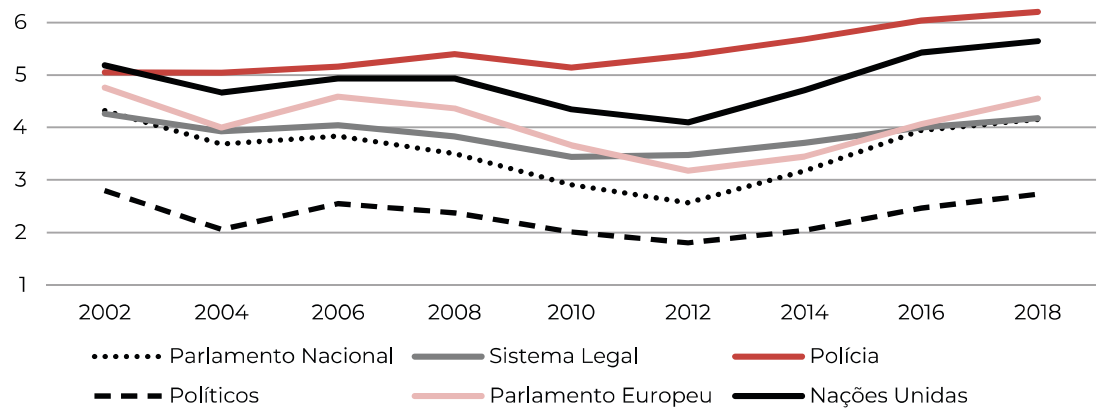
Este conjunto de perceções fornece indicações relevantes para a definição de políticas de investimento (ou intervenções a outros planos) no reforço de meios, criação ou alteração de estatutos e funções de entidades, formação/informação de determinados públicos-alvo sobre segurança do ciberespaço e sobre as ações, responsabilidades e domínios de intervenção das várias entidades públicas em contexto de cibersegurança.

No domínio das perceções sobre entidades são analisadas três dimensões: confiança, eficácia para combater o cibercrime, e preocupação sobre a utilização de dados pessoais por parte das autoridades públicas.

No que respeita à confiança dos cidadãos nas entidades nacionais e europeias envolvidas em responsabilidades legislativas, executivas e fiscalizadoras, o *European Social Survey* (ESS) publica uma série de indicadores bienais que apresentam valores recolhidos nas mesmas condições, e para os mesmos 29 países[76], para o período 2002-2018. Apesar de mais globais, e não apenas ligados ao âmbito da cibersegurança, os resultados seguintes permitem extrair conclusões robustas e abrangentes sobre a forma como tem evoluído a confiança dos portugueses nestas entidades desde 2002, e sobre o esclarecimento e objetividade dos portugueses nas respostas neste contexto. A informação retida pode ser seguidamente confrontada com perceções associáveis, já no domínio específico da cibersegurança, favorecendo (ou não) uma melhor interpretação destas, e fundamentando possíveis indicações relevantes para a elaboração de políticas públicas nesta área.

No gráfico seguinte podemos analisar a evolução ocorrida neste indicador, para Portugal.

Figura 15. Confiança nas "entidades públicas": Média dos inquéritos (Escala 0-10) – Portugal, 2018



Fonte: European Social Survey (ESS 2021)

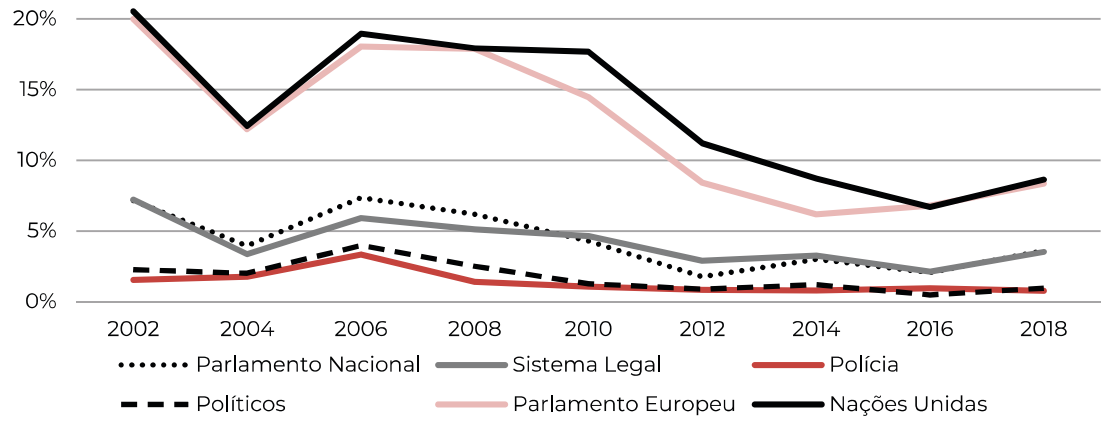
76 23 países dos atuais EU27 (faltam Grécia, Luxemburgo, Malta e Roménia), Reino Unido e mais 5 países não UE (Islândia, Montenegro, Noruega, Sérvia e Suíça).

Da análise do gráfico podemos concluir que:

- a confiança em todas as entidades aumentou nos últimos três inquéritos, i.e., seis anos consecutivos;
- a entidade "polícia" é a que tem um crescimento de confiança mais consistente desde o início da recolha de dados e está sempre no topo, destacadamente, se excluirmos o primeiro ano onde a confiança média está apenas ligeiramente abaixo da relativa às Nações Unidas;
- a confiança no sistema legal é a que se mantém mais estável ao longo de todo o período medido (à volta de 40%);
- apenas a confiança na polícia e no sistema legal não tiveram quebra acentuada e mínimos globais no inquérito de 2012;
- os portugueses tendem a confiar menos em entidades conjunturais e nacionais (políticos e parlamento nacional) comparativamente com estruturas mais estáveis, nacionais ou internacionais (polícia e Nações Unidas).

Torna-se relevante a análise da preparação dos entrevistados para esta resposta concreta, de forma a reforçar as conclusões. Pelo que podemos concluir do seguinte gráfico, onde podemos avaliar as percentagens de respostas do tipo "não sabe"/"não responde", os portugueses têm vindo, em geral, a responder mais assertivamente a estas questões (tamanhos das amostras para Portugal entre 1055 indivíduos em 2018 e 2367 em 2008).

Figura 16. Percentagem de respostas "não sabe"/"não responde" – Portugal, 2018



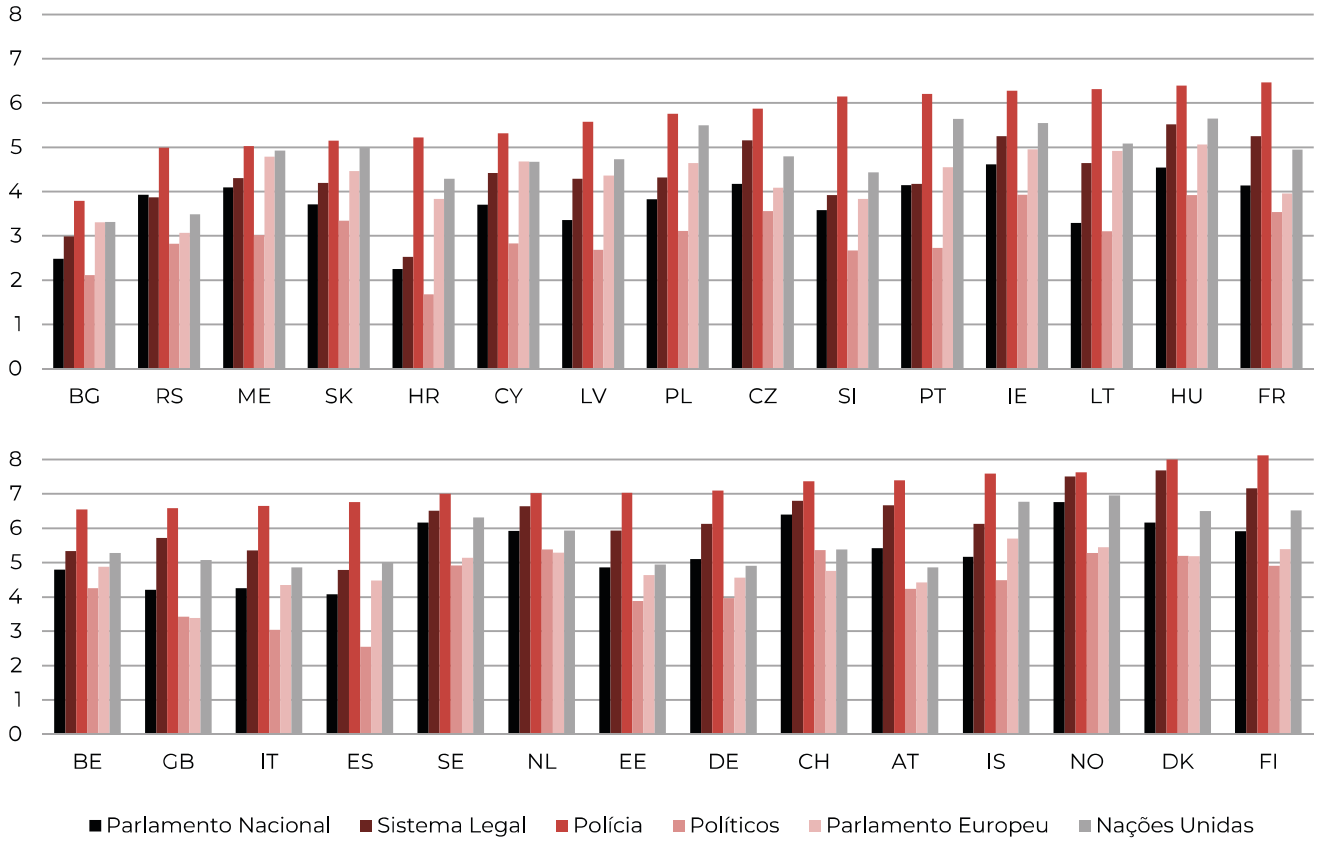
Fonte: European Social Survey (ESS 2021)

No gráfico da Figura 16 podemos confirmar:

- uma tendência global para a diminuição do peso das respostas do tipo "não sabe"/"não responde" (o desenho do inquérito prevê ainda uma alternativa adicional de recusa explícita em responder que não foi agregada);
- o grau de confiança nos políticos e na polícia corresponderam sempre às respostas onde existiram destacadamente menos dúvidas, sendo também as entidades merecedoras de menor e maior confiança, respetivamente;
- o esclarecimento nas respostas tem aumentado mais significativamente nos últimos inquéritos quanto às organizações internacionais (PE e NU) correspondendo também às entidades com maior aumento nos níveis de confiança no mesmo período.

Olhando agora para o panorama dos 29 países analisados pelo ESS em 2018, podemos verificar algumas sintonias com Portugal, por consulta à Figura 17.

Figura 17. Confiança média (de respostas assertivas na escala 0-10) nas "entidades públicas" - 2018



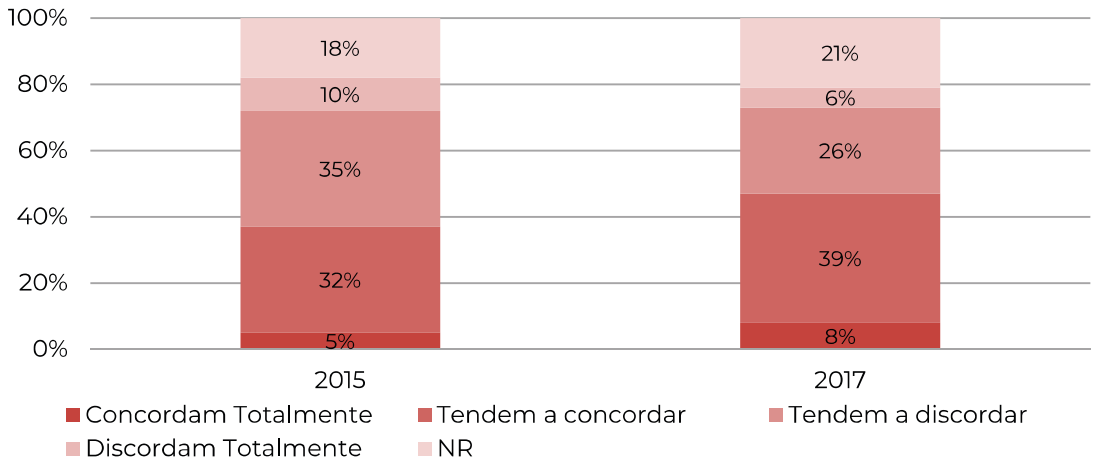
Fonte: European Social Survey (ESS 2021)

Os resultados analíticos mais evidentes revelam que:

- em todos os países, sem exceção, a polícia é a entidade merecedora de maior confiança (sempre acima dos 50% exceto na Bulgária);
- a desconfiança relativa nos políticos é global, chegando a níveis extremos em países como a Croácia (HR) e a Bulgária (BG) onde se situa por volta dos 20%;
- o sistema legal é muito frequentemente colocado na segunda posição em níveis de confiança, tendência apenas claramente contrariada na Croácia;
- os países nórdicos apresentam os maiores níveis de confiança na globalidade das entidades.

Relativamente à eficácia das entidades públicas no combate específico ao cibercrime, o Eurobarómetro contempla o estudo de diferentes indicadores neste domínio. Em primeiro lugar, na Figura 18, apresenta-se a perceção que os cidadãos têm sobre a eficácia da polícia e outras entidades públicas. Neste domínio, os únicos dados disponíveis são fornecidos pelos inquéritos de 2015 e 2017.

Figura 18. A polícia e as autoridades públicas estão a fazer o suficiente para combater o cibercrime em Portugal



Fonte: Eurobarómetro (UE 2015b, 2017b)

Na Figura 18 verificamos que, de 2015 para 2017, a percentagem de cidadãos que concordam totalmente, ou tendem a concordar, que as autoridades públicas estão a fazer o suficiente subiu de 37% para 47%, enquanto a percentagem dos que discordam desceu de 45% para 32%. As não-respostas mantiveram-se em torno dos 20%.

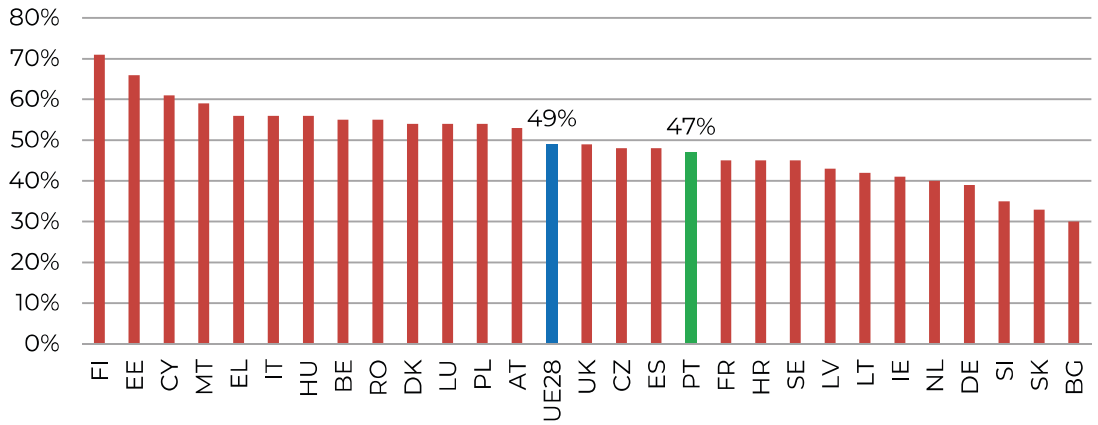
Em termos da divisão por género, idade, nível de instrução, local de residência e tipologia de utilização da Internet, analisando em detalhe os dados desagregados deste indicador no Eurobarómetro, podemos enfatizar as seguintes conclusões (úteis para o planeamento de eventuais intervenções diferenciadas em, também eventualmente diferenciados, públicos-alvo):

- **Por género** - A percentagem de concordância (total ou tendencial) entre homens e mulheres é semelhante (47% e 46%, respetivamente). A discordância é maior nos homens (34% vs 30%), havendo uma menor percentagem de não-respostas nos homens (19% vs 24%);
- **Por grupo etário** - É a geração entre os 25 e os 39 anos aquela que apresenta uma maior percentagem de concordância (61% contra 27% de discordância – 12% de não-respostas), enquanto as gerações mais novas (dos 15 aos 24 anos – 48% contra 37% - 15% de não-respostas) e a geração seguinte (dos 40 aos 54 anos – 50% contra 36% - 14% de não-respostas) apresentam uma concordância ligeiramente mais baixa. A geração mais idosa (55+ anos) é a que apresenta a menor concordância (36% contra 30%) e uma maior percentagem de não-respostas (34%), o que sugere que estão menos informados sobre o assunto;
- **Por nível de instrução** - São as pessoas que abandonaram mais cedo a escola que têm pior opinião sobre a eficiência da polícia e das autoridades públicas no combate ao cibercrime (33% de concordância contra 33% de discordância), sendo também os menos informados (34% de não-respostas). Os outros níveis de instrução (abandonaram a escola depois dos 15 anos de escolaridade, depois dos 20 anos e estudantes atuais) apresentam um comportamento semelhante (52-58% de concordância contra 32-35% de discordância e 10-14% de não-respostas);
- **Por local de habitação** - Os que apresentam maior concordância vivem em ambiente rural (49%) ou nas grandes cidades (53%), relativamente a quem habita em cidades de pequena ou média dimensão (38%). Os que menos respondem à pergunta vivem em ambiente rural ou em cidades pequenas ou médias (21% e 25%, respetivamente), em contraste com quem vive nas grandes cidades (17%);

- **Por tipologia de utilização da Internet** - São os cidadãos que utilizam serviços bancários *online*, compras *online* ou televisão *online*, os que mais consideram que as autoridades públicas fazem o suficiente para combater o cibercrime (concordâncias superiores a 60%), se bem que os resultados não sejam muito diferenciados (menor concordância de 54% em utilizadores de serviços noticiosos e jogos).

Considerando a Figura 19, comparando com os países da UE, Portugal está abaixo da média da UE28 na percentagem dos cidadãos que concordam totalmente ou tendem a concordar, apesar da diferença não ser expressiva (49% para a UE e 47% para Portugal).

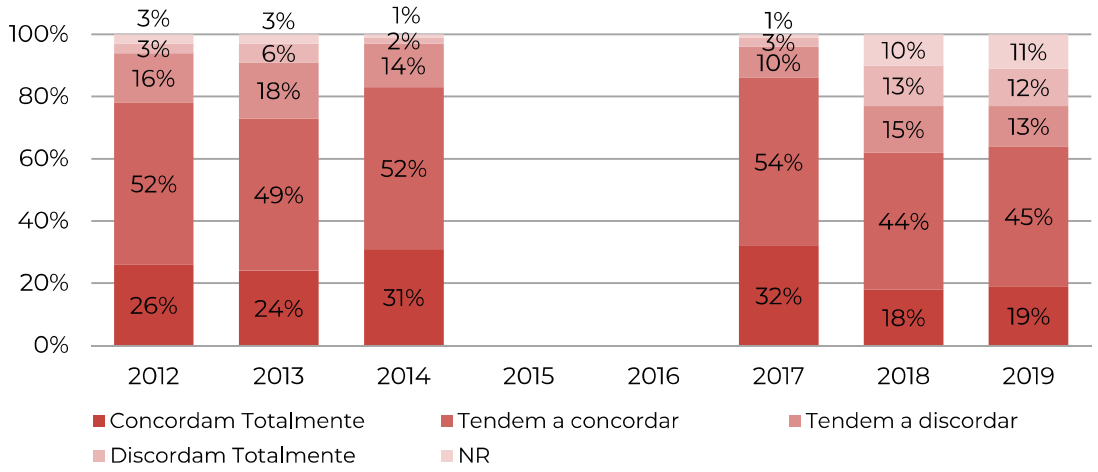
Figura 19. A polícia e as autoridades públicas estão a fazer o suficiente para combater o cibercrime, comparação europeia -2017



Fonte: Eurobarómetro (UE 2017a)

A segunda dimensão analisada neste ponto sobre cibersegurança e autoridades públicas é se os cidadãos estão preocupados se as autoridades públicas tratam e mantêm seguros os dados digitais. O Eurobarómetro recolheu dados sobre esta preocupação para os triénios 2012-2014 e 2017-2019.

Figura 20. As autoridades públicas estão a tratar de forma segura os meus dados pessoais, Portugal



Fonte: Eurobarómetro (UE 2012, 2013, 2015a, 2017a, 2019, 2020)

Na Figura 20 podemos observar que a maioria dos portugueses mostra muita ou alguma preocupação com este facto, sendo que após 2017 essa percentagem diminui de valores em torno dos 80% para valores em torno de 60%.

Esta redução não se traduziu num aumento equivalente dos portugueses que não estão preocupados e, portanto, confiam nas autoridades públicas. Na realidade os que "não sabem"/"não respondem" aumentaram de valores residuais para cerca de 10%.

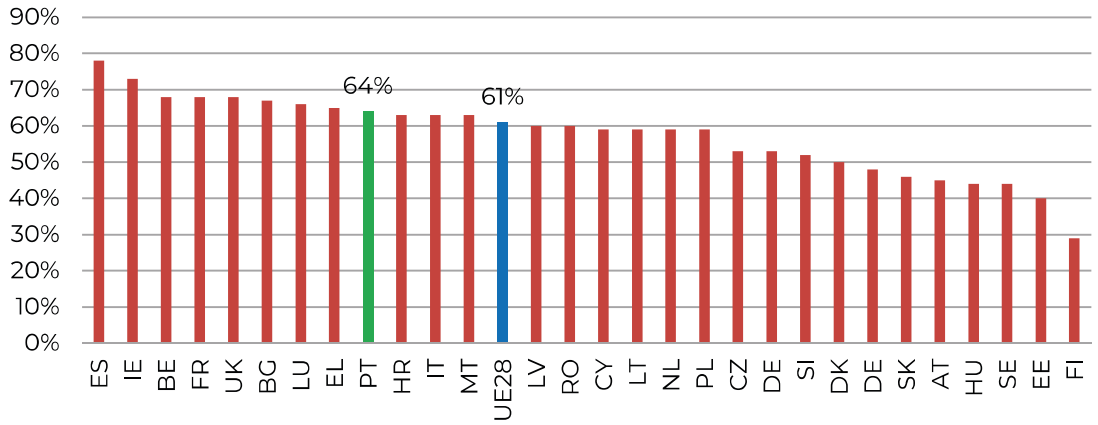
Os que não se preocupam e, portanto, confiam nas autoridades públicas têm uma oscilação, sendo cerca de 19-24% em 2012/2013, descendo para 13%-16% em 2014 e 2107 e voltando a aumentar para 28%-25% em 2018-19.

Desagregando novamente os resultados, agora apenas por género, idade, nível de instrução e local de residência podemos assinalar que:

- **Por género** - Não há grandes diferenças (66% de preocupação nos homens contra 63% de preocupação nas mulheres e uma maior percentagem de não-respostas nestas – 12% contra 8%);
- **Por idade** - São os que têm mais de 55 anos que menos se preocupam com o tratamento de dados (apenas 43%) e que menos respondem à pergunta (23% de não-respostas). Por outro lado, são os cidadãos mais jovens (entre 15 e 24 anos) os que mais se preocupam (86%);
- **Por nível de instrução** - São os que abandonaram a escola antes dos 15 anos que menos se preocupam com o tratamento de dados (apenas 38%) e que menos respondem à pergunta (22% de não-respostas). Os restantes níveis apresentam valores elevados de preocupação (entre os 80% e 85%).
- **Por local de residência** - Apesar de todos os locais apresentarem uma percentagem de cidadãos que se preocupam com o tratamento de dados pelas autoridades públicas acima dos 50%, esta percentagem é maior em ambiente urbano (pequenas e médias cidades, 71%, e grandes cidades, 69%) do que em ambiente rural (57%).

Na comparação europeia (Figura 21) verificamos que 61% dos europeus estão preocupados com a forma como as autoridades públicas tratam os seus dados pessoais. Contudo, o cenário é bastante heterogéneo oscilando entre um máximo de 78% na Espanha e um mínimo de 29% na Finlândia. Nesta comparação, Portugal está ligeiramente acima da média europeia.

Figura 21. Preocupação com o tratamento de dados *online* pelas autoridades públicas, comparação europeia – 2019



Fonte: Eurobarómetro (UE 2020)

I.3 PERCEÇÕES SOBRE RESPOSTA A AMEAÇAS

Nesta secção pretende-se avaliar a perceção dos portugueses sobre a sua própria preparação para identificar e responder adequadamente, no sentido de reportar as ocorrências de diferentes tipologias de crime no ciberespaço, bem como confrontar as suas intensões eventuais de reporte (na ausência de qualquer tipo de problema) com as suas atitudes concretas de reporte (na presença concreta de um evento que ameace a sua presença no ciberespaço). Este conjunto de perceções contribui essencialmente para a definição de políticas e práticas de formação dos utilizadores, eventualmente dirigidas a tipologias selecionadas dos mesmos, bem como podem sugerir a necessidade de reforçar alguns serviços de atendimento/tratamento dos reportes de crimes. Estes serviços devem ser diferenciados/especializados de acordo com as respetivas tipologias-alvo de incidente a responder, para uma resposta mais eficaz, e dimensionados pela previsão do volume de queixas, para uma reação de resposta mais rápida.

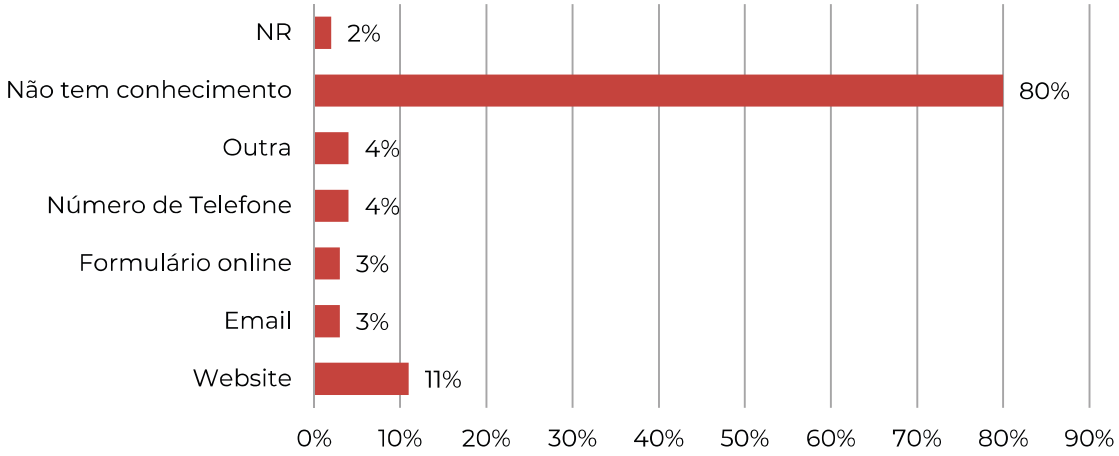
Na subsecção anterior reportou-se a confiança dos cidadãos nas autoridades públicas, quer no combate ao cibercrime, quer na forma como estas tratam os seus dados pessoais. Contudo, essa análise dá apenas uma visão da confiança, e não esclarece se os cidadãos sabem efetivamente como interagir com as autoridades públicas.

Para perceber se os cidadãos têm uma noção de como interagir com as autoridades públicas ou se estas estão a ser capazes de comunicar com os cidadãos, esta secção analisa duas dimensões para Portugal e as respetivas comparações com a UE (a que acresce o Reino Unido):

- se os cidadãos sabem como reportar cibercrime;
- no caso de serem vítimas, qual a ação que tencionam realizar para reportar o cibercrime para diferentes tipologias do mesmo, e como é que essa intenção compara com as ações realizadas por quem foi de facto vítima;

Relativamente ao primeiro indicador (nível de conhecimento de canais para reportar ciberataques) no Eurobarómetro (UE 2020) vemos que, em 2019, em Portugal, a esmagadora maioria dos cidadãos (80%) não tinha conhecimento de canais para reportar cibercrimes. Entre os que tinham conhecimento de um mecanismo, o canal mais mencionado foi a "existência de *website*" (Figura 22).

Figura 22. Conhecimento da existência de um mecanismo de reporte de cibercrimes, Portugal -2019

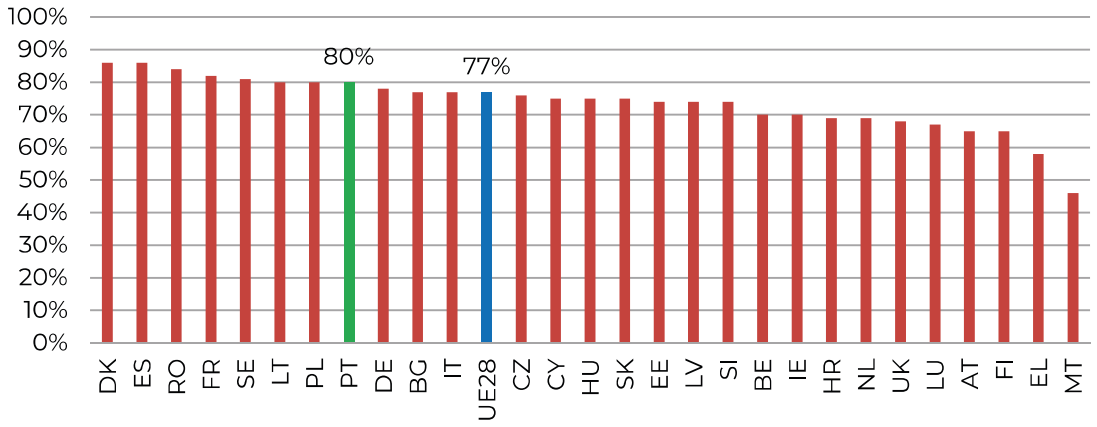


Fonte: Eurobarómetro (UE 2020)

Relativamente às diversas desagregações dos dados constantes da Figura 22 não há diferenças significativas, sendo que quem é mais velho, tem menos instrução e vive em ambiente rural tem um maior desconhecimento da existência de canais de reporte. Contudo, e de forma geral, o desconhecimento é muito elevado, mesmo entre estudantes. Quem revela menos desconhecimento sobre os canais de reporte de cibercrime são os cidadãos que acedem à Internet através da TV ou de consola de jogos, sendo que nestes dois casos a maior parte das pessoas que tem conhecimento de um mecanismo de reporte, refere a existência de um *website*.

Comparando com os países de UE e o Reino Unido (UE28) verificamos que o elevado nível de desconhecimento de como reportar cibercrimes é geral, com exceção de Malta (Figura 23). Mesmo assim, Portugal está ligeiramente acima da média europeia (80% *vs* 77%).

Figura 23. Desconhecimento da existência de um mecanismo de reporte de cibercrimes - 2019

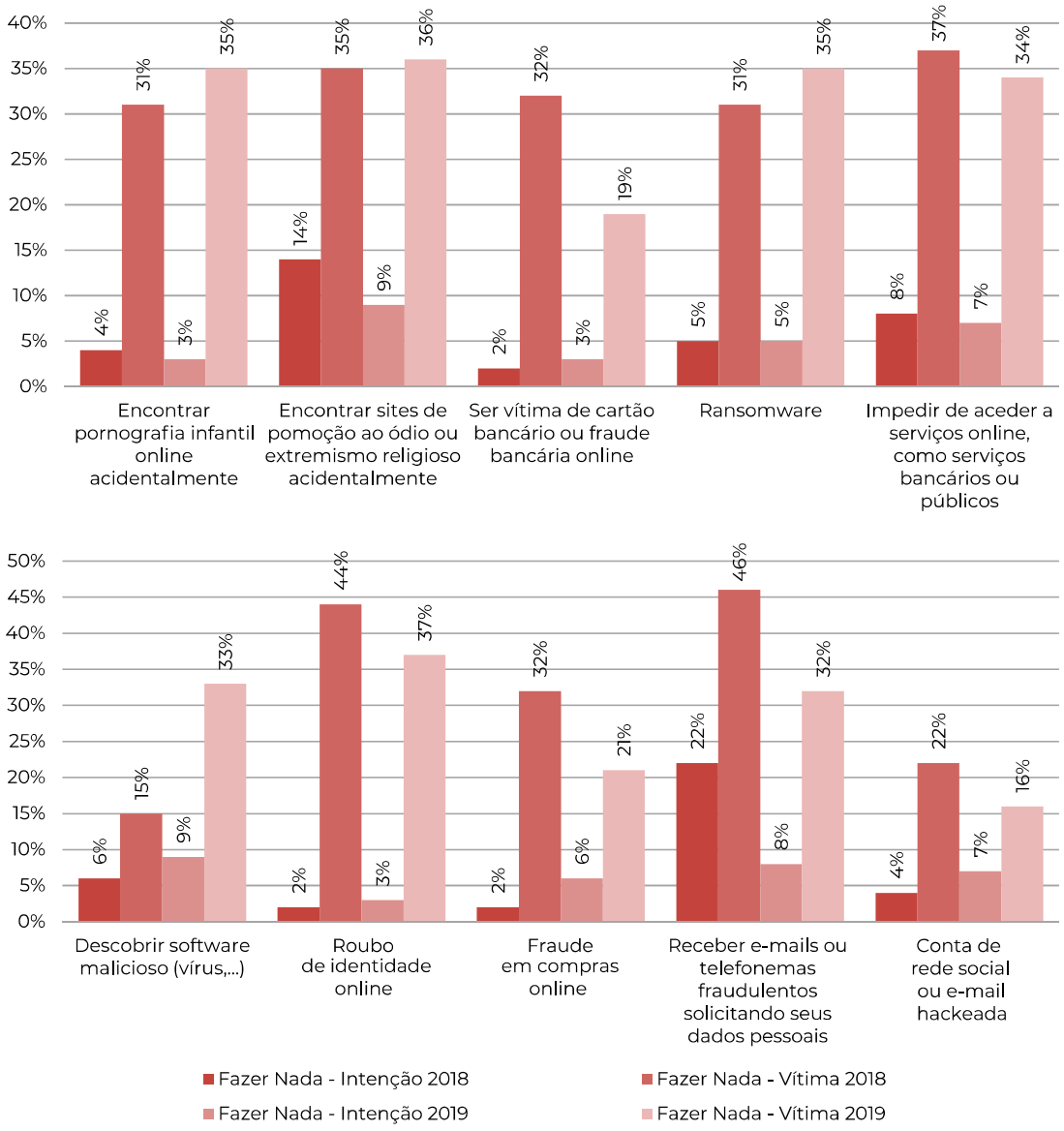


Fonte: Eurobarómetro (UE 2020)

Na comparação entre a intenção de reporte e as ações tomadas no caso de se ser vítima podemos ver na Figura 24 que, entre 2018 e 2019, não houve grandes modificações nos diversos cibercrimes com exceção do reporte relativo a receber *e-mails* ou telefonemas fraudulentos em que houve uma diminuição de 22% para 8% na intenção de não tomar nenhuma ação e de 46% para 32% na tomada de nenhuma ação no caso de ser vítima.

Contudo, de forma geral, a percentagem de cidadãos que não manifestam qualquer intenção de agir é bastante menor, em termos hipotéticos, do que quando são confrontados com o crime efetivo. Neste último caso, é consideravelmente superior a percentagem de cidadãos que não toma qualquer ação de reporte.

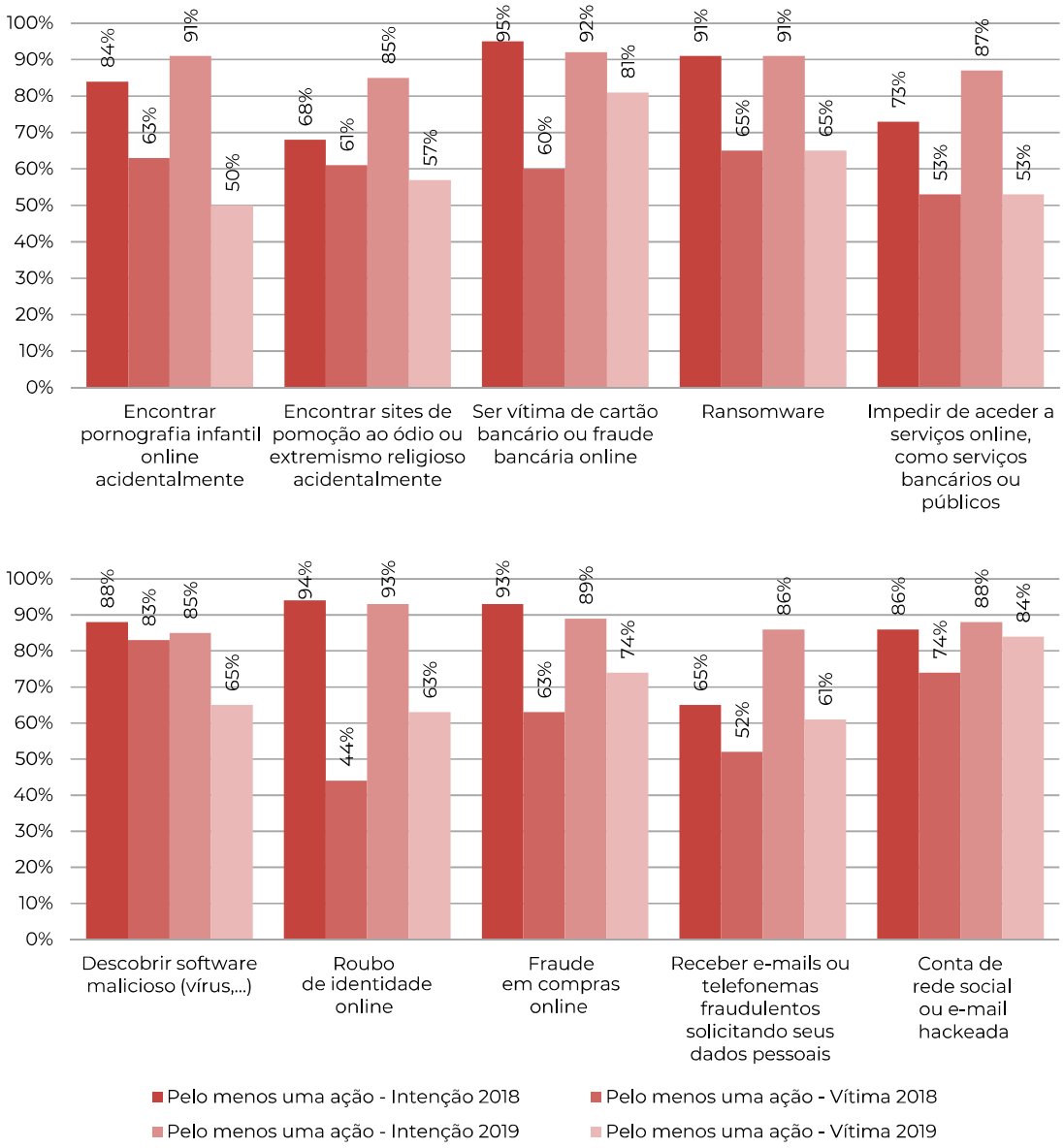
Figura 24. Proporção de não reporte de cibercrime



Fonte: Eurobarómetro (UE 2019, 2020)

Quanto à tomada de ação, confirma-se, nas Figuras 25 e 26, que a intenção de reportar é sempre bastante superior à sua concretização.

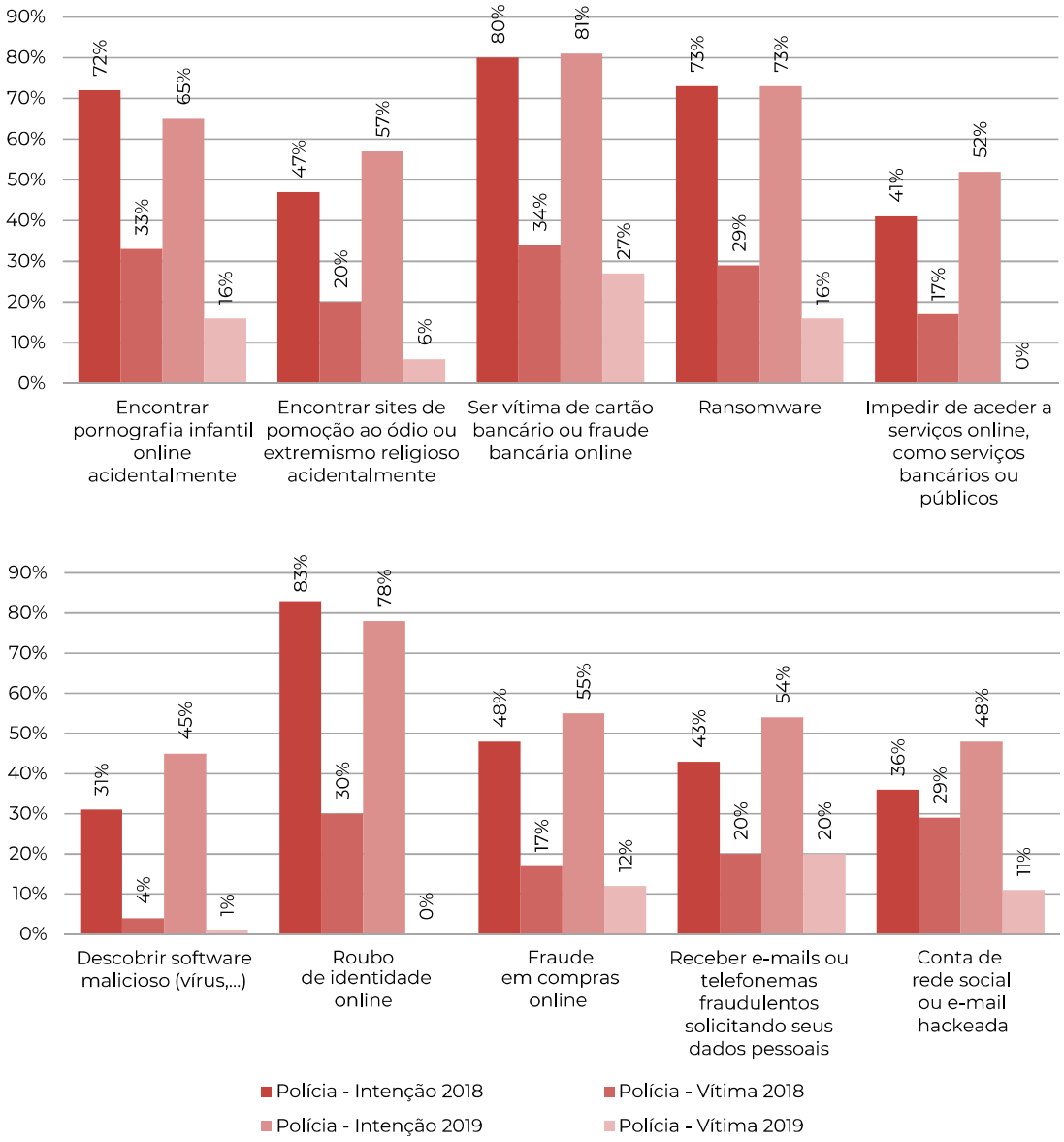
Figura 25. Proporção de reporte face ao cibercrime



Fonte: Eurobarómetro (UE 2019, 2020)

Por outro lado, a intenção de tomar uma ação e reportar à polícia é bastante semelhante em crimes bancários, *ransomware* e roubo de identidade, enquanto noutros crimes a intenção de reportar à polícia é bastante inferior relativamente a tomar ações alternativas (junto da entidade que disponibiliza os servidores, da loja *online* ou de outras entidades privadas). Contudo, quando os cidadãos são vítimas ou se deparam com o cibercrime a percentagem que reporta à polícia é sempre menor do que a dos que realizam ações alternativas, sendo que essa percentagem diminuiu de 2018 para 2019, chegando mesmo a zero em alguns casos.

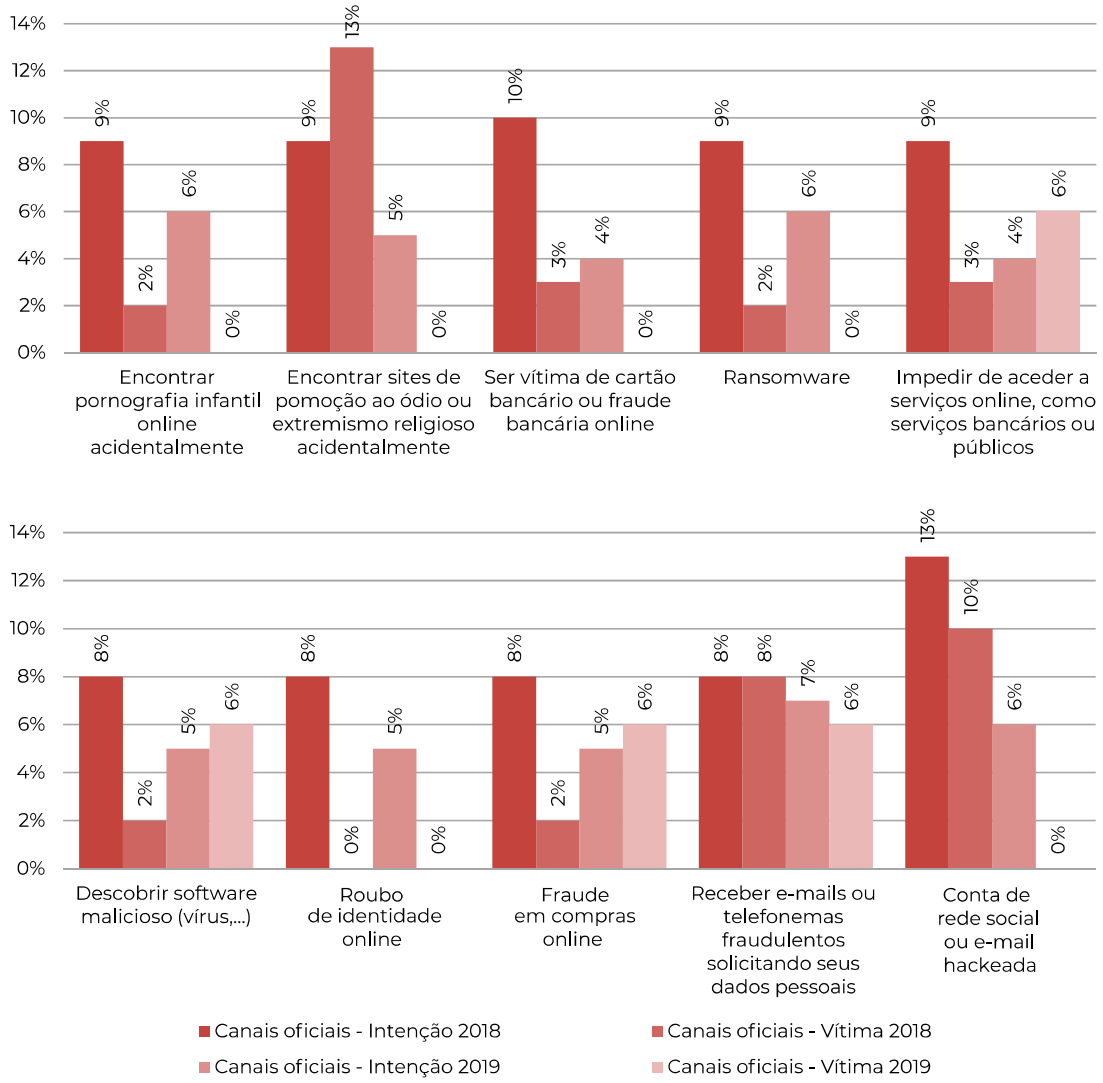
Figura 26. Proporção da intenção de reportar e do reporte de cibercrime à polícia



Fonte: Eurobarómetro (UE 2019, 2020)

A Figura 27 mostra que a percentagem dos que têm intenção ou reportam o cibercrime através de outro canal oficial que não a polícia é bastante baixa, o que mostra que há um desconhecimento geral da existência de canais próprios para reportar um cibercrime.

Figura 27. Proporção da intenção de reportar e do reporte de cibercrime por canais oficiais

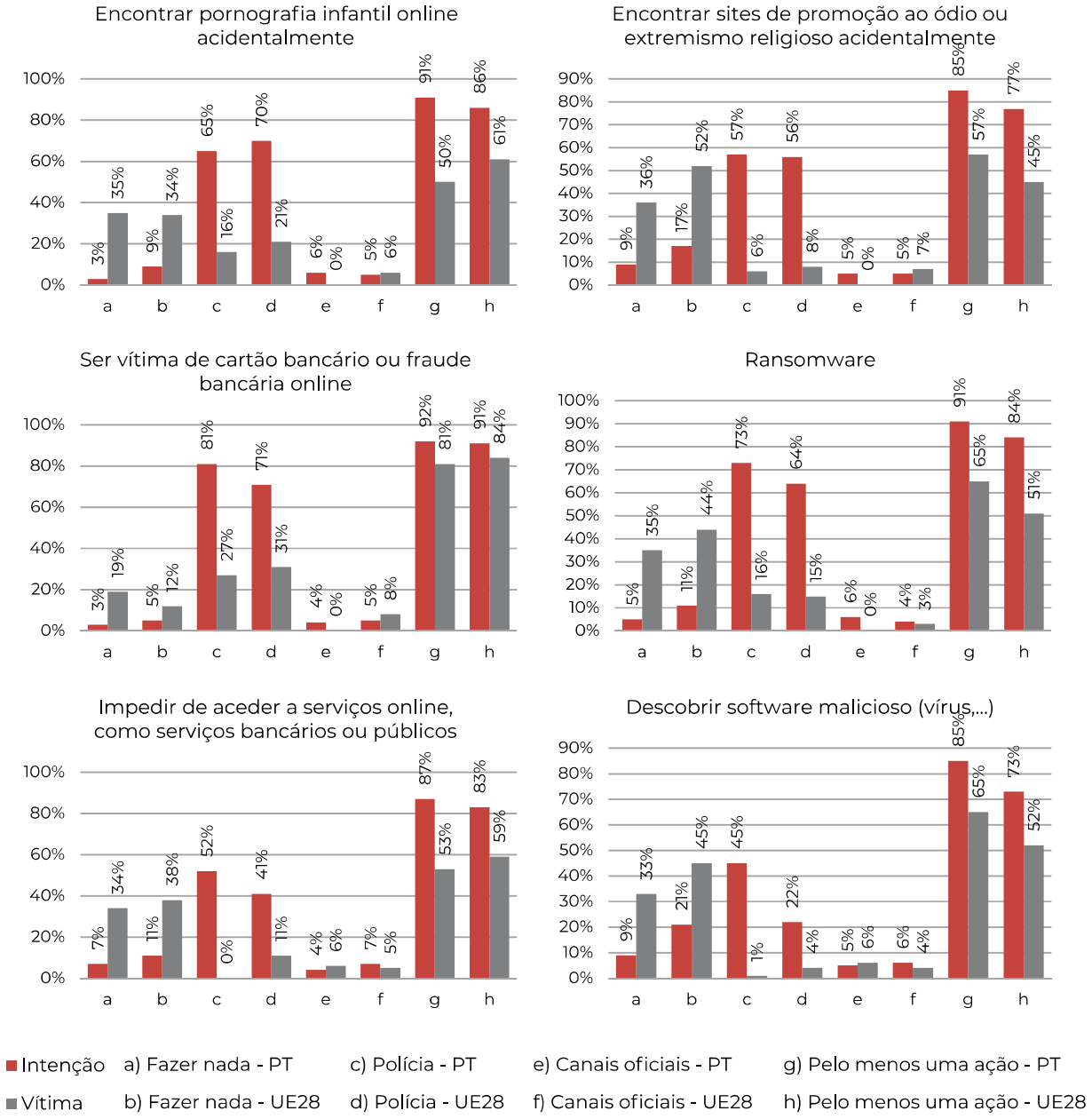


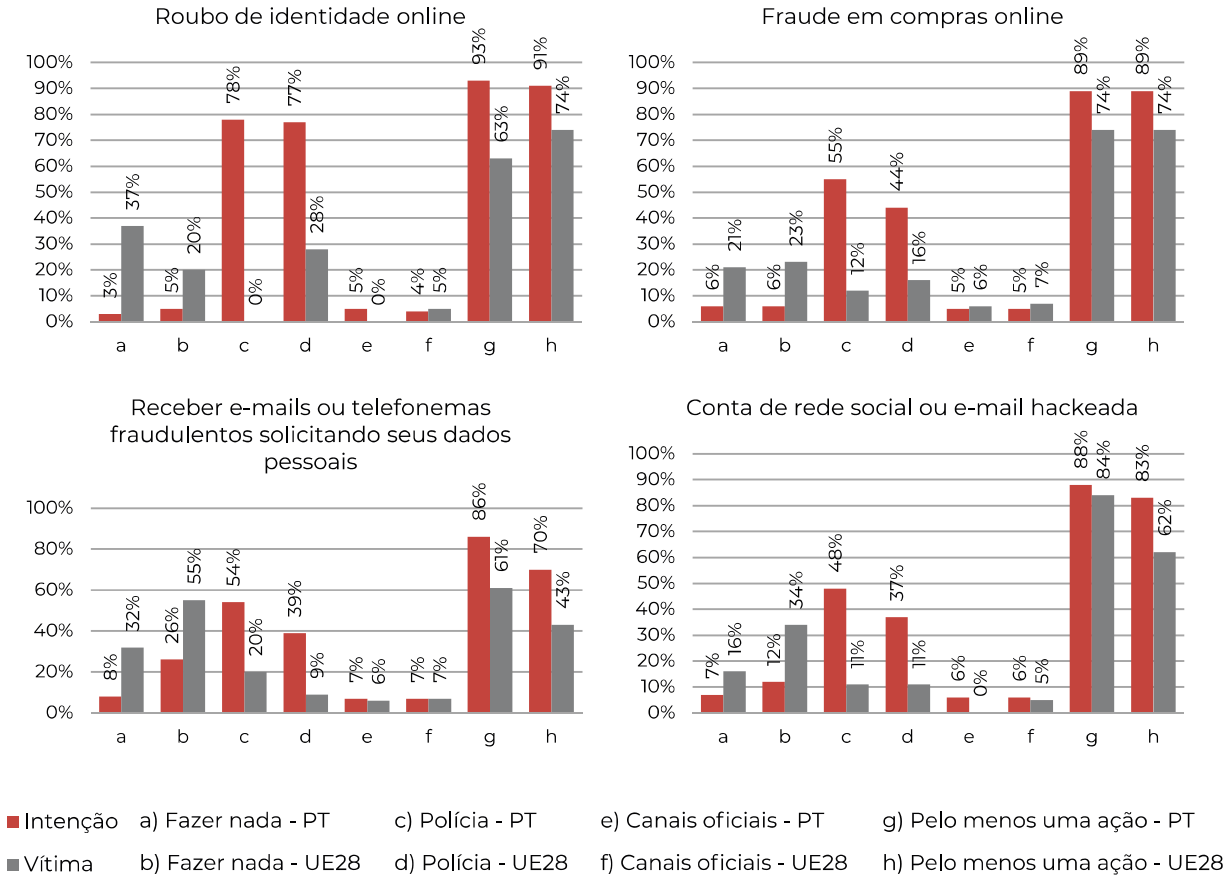
Fonte: Eurobarómetro (UE 2019, 2020)

Em conclusão, o baixo reporte à polícia ou através de canais oficiais demonstra que, apesar das intenções, quando confrontados com o cibercrime, os cidadãos desconhecem, ou têm menos confiança nas autoridades públicas, confiando mais em entidades privadas com quem têm maior proximidade, seja o banco, a loja *online* ou as empresas fornecedoras de Internet.

Da análise da Figura 28, comparando com a UE em 2019 (UE28), verificamos que o cenário em Portugal é em tudo idêntico ao do resto da Europa: altas taxas de intenção de reporte de crime quando comparadas com as taxas de reporte efetivo; uma menor taxa de reporte à polícia do que a canais alternativos; e um desconhecimento da existência de canais oficiais de reporte. Estes dados confirmam algumas conclusões já apresentadas no *Relatório Sociedade 2020* (CNCS 2020d).

Figura 28. Proporção da intenção de reportar e do reporte de cibercrimes à polícia - comparação de Portugal com a UE28





Fonte: Eurobarómetro (UE 2019, 2020)

I.4 PERCEÇÕES SOBRE IMPACTO DAS *FAKE NEWS*

Apesar de as *fake news* estarem relacionadas com o assunto global da perceção pública, elas apresentam especificidades que justificam uma análise isolada sobre o fenómeno porque estas terão impacto independente, direto, e possivelmente negativo, sobre a aferição das perceções dos cidadãos.

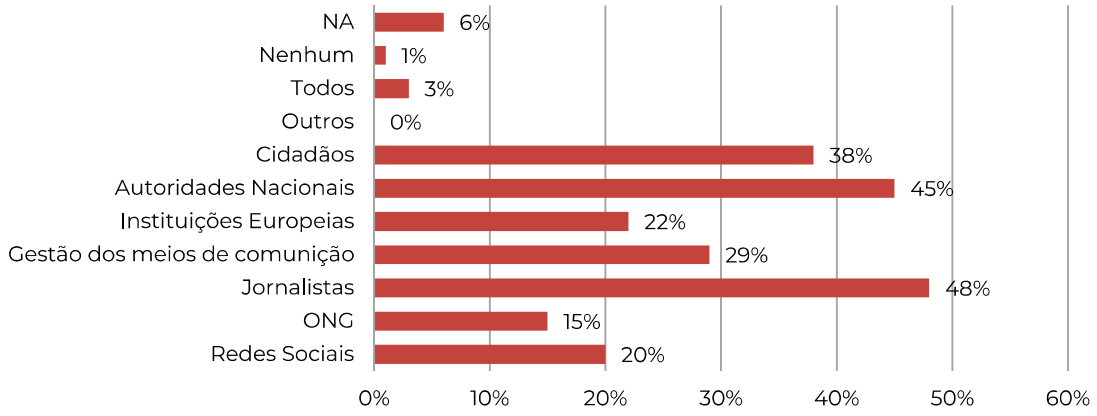
Esta secção pretende contribuir para a tomada de decisões fundamentadas na definição de políticas públicas para mitigar o efeito da disseminação de *fake news*, sendo importante avaliar: o grau de preparação da sociedade para detetar *fake news*; se são conhecidos os canais de ajuda e/ou denúncia e como se utilizam; e a quem se atribui a responsabilidade de impedir a disseminação das mesmas. Estes serão os principais indicadores agora analisados.

Nesta dimensão analisa-se primeiramente quem a sociedade considera responsável pelo controle da disseminação de *fake news* com base no inquérito do Eurobarómetro (UE 2018), decompondo essa análise por idade, nível de instrução, local de residência para Portugal, e comparando com os restantes países da UE.

Numa segunda fase é apresentada a correlação dos indicadores anteriores com a exposição às *fake news*, assim como com a perceção do impacto que estas têm na sociedade.

Da Figura 29 verifica-se que, em Portugal, os cidadãos consideram que os três atores que devem impedir a disseminação de *fake news* são os "Jornalistas", "Autoridades Nacionais" e os próprios "Cidadãos", dando menos relevo a outros atores, nomeadamente às instituições europeias.

Figura 29. Instituições e atores que devem agir para impedir a disseminação de *fake news - 2018*



Fonte: Eurobarómetro (UE 2018)

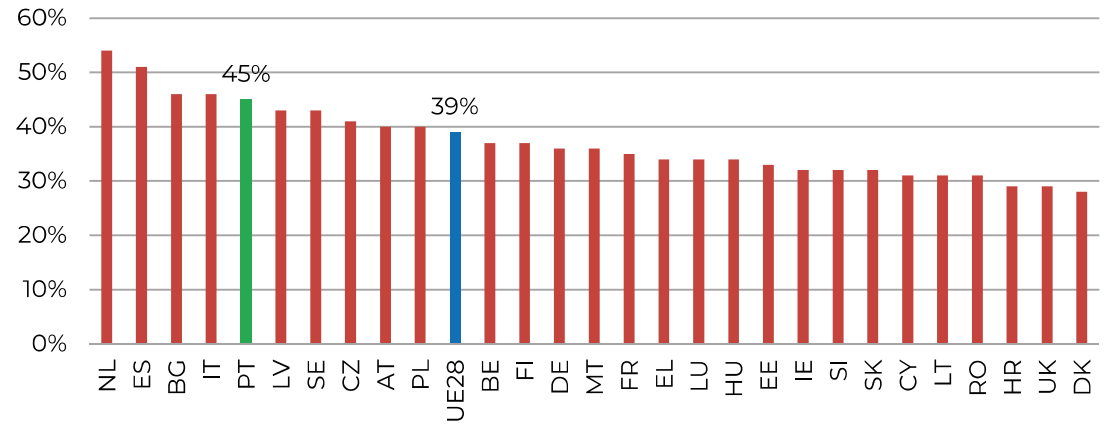
Fazendo a desagregação e análise dos dados da Figura 29 por género, idade, nível de instrução e local de residência, é possível concluir que:

- **Por género** - Não há grande diferença nas respostas entre homens e mulheres.
- **Por idade** - Os cidadãos com menos de 25 anos consideram que a responsabilidade deve ser dada aos jornalistas (54%) e cidadãos (52%), enquanto os mais velhos têm uma maior percentagem de não-respostas (12%), o que pode ser revelador de menor informação sobre o assunto.
- **Por nível de instrução** - Os que estudaram até mais tarde atribuem maior responsabilidade às autoridades nacionais (54%). Já os que têm menor nível de instrução e os estudantes constituem os dois grupos que menos as responsabilizam (33% e 42% respetivamente). A diferença entre estes dois últimos grupos é que os estudantes dão maior peso aos cidadãos e jornalistas (55% em ambos os casos) enquanto os menos instruídos revelam maior desconhecimento com um maior número de não-respostas (13%).
- **Por local de residência** - Quem vive em maiores aglomerações populacionais tem um menor nível de não-respostas (3%).

Em síntese, os cidadãos portugueses consideram que as autoridades nacionais devem ser um ator relevante para impedir a disseminação de *fake news*, juntamente com os jornalistas e cidadãos. Contudo, os mais jovens dão maior ênfase às responsabilidades individuais (jornalistas e cidadãos), em contraste com as autoridades nacionais. Por outro lado, os mais idosos e habitantes em espaços rurais apresentam a maior percentagem de não-respostas, o que pode refletir a menor informação destes grupos.

A Figura 30 compara a relevância dada às autoridades nacionais pelos cidadãos dos países europeus.

Figura 30. Importância das Autoridades Nacionais, comparação europeia -2018



Fonte: Eurobarómetro (UE 2018)

Numa análise comparativa, Portugal é dos países em que os cidadãos mais consideram que as autoridades nacionais devem ter um papel ativo no controlo de disseminação das *fake news*, apenas suplantado pelos Países Baixos, Espanha, Bulgária e Itália, mas muito acima da média da UE28.

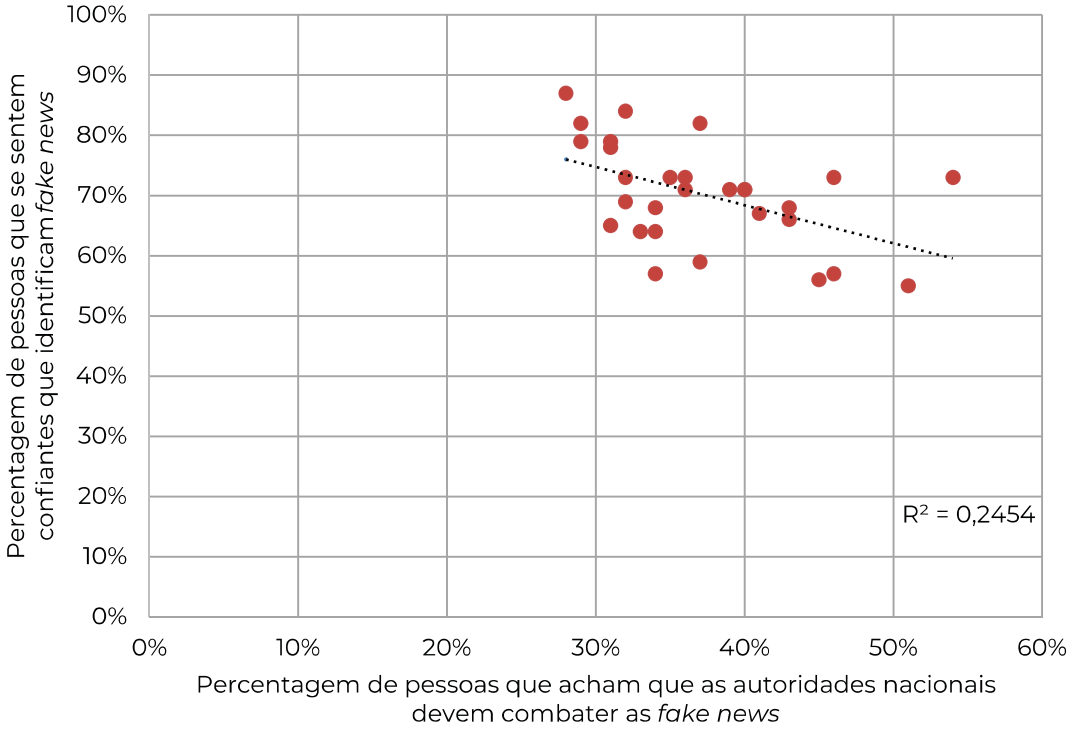
Da análise dos dados do Eurobarómetro verificamos que as diferenças observadas entre países europeus sobre a importância dada às autoridades nacionais no combate às *fake news* não está significativamente relacionada nem com a exposição às mesmas, nem com o facto de as *fake news* serem consideradas um problema para o país ou ameaça para a democracia.

A única variável que se relaciona com a importância dada às autoridades nacionais é a perceção de "se conseguir identificar *fake news*". Assim, quanto mais os cidadãos de um país têm a perceção de que conseguem identificar *fake news* menos relevância dão às autoridades nacionais no combate às mesmas (Figura 31). Esta tendência global na perceção dos europeus pode ser interpretada como um indicador de segurança/insegurança:

- por parte dos que se sentem menos preparados para identificar *fake news,* um apelo a uma maior intervenção das autoridades nacionais, mais próximas da realidade de cada país, no sentido de prevenir/mitigar os efeitos mais perturbadores e negativos das f*ake news*;
- por parte dos que se sentem mais aptos a reconhecer e relevar o conteúdo das *fake news*, uma maior segurança que permite aceitar que exista uma espécie de autorregulação e atenuação do efeito das *fake news* pelos próprios envolvidos na produção, divulgação e consumo das mesmas (jornalistas, redes sociais, cidadãos e outros intervenientes no processo global de disseminação).

Em ambas as perspetivas parecem óbvias as vantagens de um maior esclarecimento dos destinatários selecionados pelo fenómeno (cidadãos ou organizações em geral ou grupos selecionados de interesse). Esse desígnio pode ser atingido, numa perspetiva nacional, através de ações de formação/informação dirigidas ao público em geral, ou a setores/estratos específicos de particular risco. Essas ações potenciariam a capacidade de discernimento na aceitação do que é divulgado, em função de "onde" e "como" é divulgado, e forneceriam eventualmente algumas pistas sobre precauções a ter para identificação da *fake news* típica, bem como de fenómenos derivados (negação da realidade, testemunhos ilegítimos, etc.).

Figura 31. Importância dada às autoridades nacionais vs confiança que identifica *fake news* - 2018



Fonte: Eurobarómetro (UE 2018)

J

NOTAS CONCLUSIVAS

De forma geral, as estratégias adotadas em Portugal têm acompanhado os objetivos e orientações estratégicas de segurança da UE. A Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada em 2019, é já o produto da execução e revisão da primeira estratégia adotada em 2015. Simultaneamente, tem vindo a ser executado um Plano de Ação que, na sua última revisão, inclui 667 atividades propostas por 67 serviços e organismos da Administração Pública, e tem contado com o envolvimento de organizações da sociedade civil, para o período de 2019-2021.

Para além da Estratégia Nacional de Segurança do Ciberespaço e do respetivo Plano de Ação, este relatório identificou um conjunto de outras estratégias, planos, programas e iniciativas nacionais, temáticas e setoriais, que é crucial considerar para obter um panorama geral das políticas públicas de cibersegurança em Portugal.

Observa-se que a interpenetração e transversalidade da cibersegurança nas mais variadas políticas públicas nacionais, juntamente com a rápida e ambiciosa evolução da arquitetura europeia de cibersegurança, tende a edificar um sistema cada vez mais complexo e desafiante em termos de coordenação política, execução e monitorização.

Cumpre ao CNCS acompanhar — desde a fase da formulação à da implementação, e monitorização da execução — estes diferentes instrumentos de política pública (estratégias, planos de ação, programas, ...) e a forma como promovem, defendem e salvaguardam as múltiplas e complexas facetas da cibersegurança.

Em simultâneo, é desejável que na sua trajetória de maturação futura, a elaboração de políticas públicas de cibersegurança pondere a coordenação das novas com as já existentes para evitar maior fragmentação.

Verifica-se uma aposta crescente na transição digital que nos proporciona diversas vantagens funcionais, mas que comporta riscos acrescidos no domínio da cibersegurança, o que suscita a preocupação de que o investimento dedicado à transição digital se sustente também ao nível dos recursos humanos alocados à cibersegurança, numa proporção alinhada com as necessidades e exigências decorrentes do ambiente estratégico.

Constata-se a existência de uma oferta significativa de recursos de formação e de sensibilização em matérias de cibersegurança, cuja difusão reforçada é fundamental para fomentar uma maior consciencialização e comportamentos mais seguros no ciberespaço por parte de cidadãos e profissionais. Dadas as características diferenciadoras dessa oferta formativa, revela-se importante organizar e centralizar essa oferta de acordo com os destinatários, objetivos e grau de exigência de forma a guiar os cidadãos em geral na escolha do tipo de curso adequado ao seu perfil e aos seus objetivos. Afigura-se ainda pertinente a criação de mecanismos de certificação de oferta formativa, particularmente de oferta não diretamente promovida pelo CNCS, de forma a fomentar e garantir a sua qualidade.

Existe um hiato significativo entre a intenção dos cidadãos em reportar um potencial crime informático e a sua concretização quando dele são vítimas. Importará aprofundar a análise de forma a compreender melhor os fundamentos de tal hiato, e atuar de forma a atenuar — ou, se possível, eliminar — as barreiras que venham a ser identificadas.

Verifica-se um elevado grau de desconhecimento, entre os que sofreram efetivamente um cibercrime, sobre a existência e a identificação de canais oficiais de reporte, bem como uma preferência por canais ditos alternativos (fornecedores de serviços de Internet, por exemplo) face aos órgãos de polícia criminal. Assim sendo, afigura-se relevante melhorar a divulgação dos canais adequados a esse reporte.

O quadro estratégico, institucional e legal existente a nível europeu sugere ser esperada, num futuro próximo, uma resposta coletiva cada vez mais integrada, que suplante de forma mais eficiente o trabalho realizado separadamente pelas diferentes comunidades de cibersegurança nos diferentes Estados-Membros (forças policiais, civis, diplomacia, parceiros do setor privado, etc.).

A cibersegurança exige um esforço contínuo, reforçado e colaborativo, enquadrado por um conjunto robusto de políticas públicas. Sendo certo que é sempre possível melhorar, Portugal surge atualmente bem posicionado nos principais *rankings* internacionais da área.

K

NOTAS METODOLÓGICAS

Para a identificação do quadro legal e institucional de referência nacional em cibersegurança que serviu de base à elaboração, desde logo, da secção F, foi efetuada uma análise documental do Diário da República (DR). Assim, foi efetuada uma pesquisa sistemática dos termos "cibersegurança", "cibercrime", "cibercriminalidade", "ciberdefesa" e "ciberameaça", na 1ª Série do DR, até ao dia 15 de setembro de 2021. A partir da lista de atos normativos obtida, selecionaram-se os diplomas fundamentais também para a identificação dos instrumentos de política pública (estratégias, planos, programas, etc.) que estão na base da elaboração das secções G (Estratégias) e H (Programas Públicos). Para a construção destas duas secções (G e H) foram ainda consultadas a página *web* do CNCS (nomeadamente para pesquisa dos anteriores relatórios do Observatório de Cibersegurança), bem como outras páginas oficiais associadas às estratégias e programas alvo de análise.

Na secção H.2 são apresentados dados e gráficos que resultam de uma escolha dos autores do relatório para cada indicador associado às medidas do PATD, para efeitos de monitorização de impacto, dados esses disponibilizados pelo Banco Mundial, Eurostat e Direção-Geral de Estatísticas da Educação e Ciência (DGEEC).

Na secção I (Perceções) são analisados dados recolhidos no âmbito de sondagens do Eurobarómetro e do *European Social Survey* (ESS).

REFERÊNCIAS

Aaltola, K., e Ruoslahti, H. (2020). Societal Impact Assessment of a Cyber Security Network Project. *Information e Security: An International Journal*, *46*(1), 53–64 https://doi.org/10.11610/isij.4604

Bahuguna, A., Bisht, R. K., e Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*, *29*(5), 250–266. https://doi.org/10.1080/19393555.2020.1767239

Banco Mundial. (2020). Secure Internet Servers (per 1 million people) 2010-2020. Banco Mundial. https://data.worldbank.org/indicator/IT.NET.SECR (consultado em 30/10/2021)

Bârgăoanu, A., e Radu, L. (2018). Fake News or Disinformation 2.0 - Some Insights into Romanians' Digital Behaviour. *Romanian Journal of European Affairs*, *18*(1), 24–38. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3296922

Bossomaier, T., D'Alessandro, S., e Bradbury, R. (2020). *Human Dimensions of Cybersecurity*. Boca Raton, FL: CRC Press.

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, *7*(1), 1–12. https://doi.org/10.1093/cybsec/tyab001

Burdon, M., Lane, B., e von Nessen, P. (2012). Data breach notification law in the EU and Australia – Where to now? *Computer Law e Security Review*, *28*(3), 296–307. https://doi.org/10.1016/j.clsr.2012.03.007

Burkhardt, J. M. (2017). History of fake news. *Library Technology Reports*, *53*(8), 5–9.

Burstein, P. (2020). The Influence of Public Opinion and Advocacy on Public Policy: Controversies and Conclusions. In T. Janoski, C. de Leon, J. Misra, e I. William Martin (Eds.), *The New Handbook of Political Sociology* (1st ed., pp. 738–760). Cambridge University Press. https://doi.org/10.1017/9781108147828.029

Cains, M. G., Flora, L., Taber, D., King, Z., e Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/risa.13687

Calderaro, A., e Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Clark, D., Berson, T., e Lin, H. (Eds.). (2014). *At the nexus of cybersecurity and public policy: Some basic concepts and issues*. Washington, DC: The National Academies Press.

CNCS. (2019a). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf (consultado em 30/10/2021)

CNCS. (2019b). *Quadro Nacional de Referência para a Cibersegurança*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf (consultado em 30/10/2021)

CNCS. (2020a). *Arquitetura de Segurança das Redes e Sistemas de Informação (Requisitos Técnicos)*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/sama2020-rasrsi-cncs.pdf (consultado em 30/10/2021)

CNCS. (2020b). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023: Relatório de avaliação da execução 2019*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/relatorioavaliacaoexecucao2019-ago2020.pdf
(consultado em 30/10/2021)

CNCS. (2020c). *Relatório Cibersegurança em Portugal – Ética e Direito 2020*. Centro Nacional de Cibersegurança. https://www.cncs.gov.pt/pt/relatorio-etica-e-direito/
(consultado em 30/10/2021)

CNCS. (2020d). *Relatório Cibersegurança em Portugal – Sociedade 2020*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/pt/relatorio-sociedade-2020/ (consultado em 30/10/2021)

CNCS. (2020e). *Relatório Riscos e Conflitos 2020*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/pt/relatorio-riscos-conflitos-2020/ (consultado em 30/10/2021)

CNCS. (2021a). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023: Plano de Ação com execução*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/ensc2019-2023-pa-2019-2020-2021-execucao2020-mai21.pdf (consultado em 30/10/2021)

CNCS. (2021b). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023: Relatório de avaliação da execução 2020*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/relatorioavaliacaoexecucao2020-fev2021.pdf
(consultado em 30/10/2021)

CNCS. (2021c). *Relatório Riscos e Conflitos 2021*. Centro Nacional de Cibersegurança.
https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancа-cncs.pdf (consultado em 30/10/2021)

Correia, P. M. A. R., e Santos, S. I. da S. (2018). A ação do Estado em matéria de cibersegurança: Estudo de perceções no caso português. *Simbiótica*, *5*(2), 1–20.
http://dx.doi.org/10.47456/simbitica.v5i2.23142

Correia, P. M. A. R., Santos, S. I. da S., e Bilhim, J. A. de F. (2017). Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime. *Sociologia : Revista Da Faculdade de Letras Da Universidade Do Porto*, *33*(0), 95–113. http://aleph.letras.up.pt/index.php/Sociologia/article/view/2822 (consultado em 30/10/2021)

CTIC. (2020). *Estratégia Cloud para a Administração Pública em Portugal*. CTIC - Conselho para as Tecnologias de Informação e Comunicação na Administração Pública. https://tic.gov.pt/documents/37177/0/CTIC+Estrate%CC%81giaCloud+-+novembro2020.pdf (consultado em 30/10/2021)

de Bruijn, H., e Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

DGEEC. (2021a). Inquérito à Utilização das Tecnologias da Informação e Comunicação na Administração Pública Central e Regional - IUTICAP 2020. Direção-Geral de Estatísticas da Educação e Ciência. https://www.dgeec.mec.pt/np4/12.html (consultado em 30/10/2021)

DGEEC. (2021b). Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais - IUTICCM 2020. Direção-Geral de Estatísticas da Educação e Ciência. https://www.dgeec.mec.pt/np4/12.html (consultado em 30/10/2021)

Dunn Cavelty, M., e Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

E-Governance Academy. (2021). National Cyber Security Index (NCSI). e-Governance Academy. https://ncsi.ega.ee/ (consultado em 30/10/2021)

Economist Intelligence Unit, e Booz Allen Hamilton. (2011). *Cyber power index*. Booz Allen Hamilton.

el Kettani, M. D. E., e Debbagh, T. (2008). NCSec: a national cyber security referential for the development of a code of practice in national cyber security management. In *ICEGOV'08 - 2nd International Conference on Theory and Practice of Electronic Governance (ICEGOV 2008)* (pp. 373–380). Cairo, Egypt: ACM.

EMGFA. (2019). *Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2018-2021 (versão 2)*. Gabinete do Chefe do Estado-Maior-General das Forças Armadas. https://www.emgfa.pt/Documents/2019/DiretivaEstrategicaEMGFA-2018-2021_Ver.2.pdf (consultado em 30/10/2021)

ESS. (2021). European Social Survey – Rounds 2002 to 2018. European Social Survey. https://www.europeansocialsurvey.org/data/ (consultado em 30/10/2021)

Eurostat. (2021a). Security incidents and consequences [isoc_cisce_ic]. Eurostat. https://ec.europa.eu/eurostat/web/products-datasets/product?code=isoc_cisce_ic (consultado em 30/10/2021)

Eurostat. (2021b). Security policy: measures, risks and staff awareness [isoc_cisce_ra]. Eurostat. https://ec.europa.eu/eurostat/web/products-datasets/product?code=isoc_cisce_ra (consultado em 30/10/2021)

Eurostat. (2021c). Security related problems experienced when using the Internet [isoc_cisci_pb]. Eurostat. https://ec.europa.eu/eurostat/web/products-datasets/product?code=isoc_cisci_pb (consultado em 30/10/2021)

Furlong, S. R., e Kraft, M. E. (2021). *Public Policy: Politics, Analysis, and Alternatives* (7th ed.). Thousand Oaks, California: CQ Press.

Governo Português. (2018). *Programa Nacional de Reformas 2016-2022 (Atualização de abril 2018)*. República Portuguesa / XXI Governo Constitucional. https://www.portugal.gov.pt/upload/ficheiros/i007132.pdf (consultado em 30/10/2021)

Governo Português. (2019). *Programa do XXII Governo Constitucional 2019-2023*. República Portuguesa / XXII Governo Constitucional. https://www.portugal.gov.pt/gc22/programa-do-governo-xxii/programa-do-governo-xxii-pdf.aspx (consultado em 30/10/2021)

Hathaway, M. (2015). *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies.

Holcomb, J. F. (2004). Managing Strategic Risk. Em J. B. Bartholomees (Ed.), *US Army War College Guide to National Security Policy and Strategy* (pp. 119–132). Carlisle, PA: Strategic Studies Institute of the US Army War College. https://www.jstor.org/stable/pdf/resrep12116.8.pdf (consultado em 30/10/2021)

Holton, N., e Furnell, S. (2020). Assessing the provision of public-facing cybersecurity guidance for end-users. In *2020 IEEE 6th International Conference}on Collaboration and Internet Computing (CIC)* (pp. 161–168). https://doi.org/10.1109/CIC50333.2020.00028

ITU. (2021). Global Cybersecurity Index 2020. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (consultado em 30/10/2021)

ITU e ABIresearch. (2015). *Global Cybersecurity Index e Cyberwellness Profiles*. Geneva: International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (consultado em 30/10/2021)

Jayawardane, S., Larik, J., e Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*. Policy Brief 17. The Hague, Netherlands. https://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf (consultado em 30/10/2021)

Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab009

Korea Internet and Security Agency. (2008). Development of National Information Security Index. In *ITU Regional Cybersecurity Forum*. Brisbane, AU. https://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/weon-national-information-security-index-brisbane-july-08.pdf (consultado em 30/10/2021)

Kostyuk, N., e Wayne, C. (2021). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*, *6*(2), ogz077. https://doi.org/10.1093/jogss/ogz077

Lee, C. S., e Kim, J. H. (2020). Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. *Computers & Security*, *97*, 101995. https://doi.org/10.1016/j.cose.2020.101995

Manjikian, M. (2021). *Introduction to Cyber Politics and Policy*. Los Angeles, CA: Sage, CQ Press.

Mărcuţ, M. (2020). *The Governance of Digital Policies: Towards a New Competence in the European Union*. Springer Nature.

MDN. (2013). *Conceito Estratégico de Defesa Nacional*. Ministério da Defesa Nacional. https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf (consultado em 30/10/2021)

Min. Planeamento. (2021). *Plano de Recuperação e Resiliência*. Ministério do Planeamento. https://recuperarportugal.gov.pt/wp-content/uploads/2021/10/PRR.pdf (consultado em 30/10/2021)

Morillas, P. (2020). *Strategy-Making in the EU: From Foreign and Security Policy to External Action*. Palgrave Macmillan.

NATO. (2019). *Factsheet - NATO Cyber Defence*. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf (consultado em 30/10/2021)

Obiam, S. C. (2021). Democracy, Public Opinion, and Public Policy Making in Rivers State. *Journal of Research in Humanities and Social Science*, 9(3), 8.

ONU. (2013). *The Cyber index – International security trends and realities*. United Nations. https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (consultado em 30/10/2021)

Pollack, M. A. (2015). Theorizing EU Policy-Making. In H. Wallace, M. A. Pollack, e A. R. Young (Eds.), *Policy-Making in the European Union* (7th ed., pp. 12–45). Oxford: Oxford University Press.

Quandt, T., Frischlich, L., Boberg, S., e Schatto-Eckrodt, T. (2019). Fake news. *The International Encyclopedia of Journalism Studies*, 1–6.

Sarri, A., Kyranoudi, P., Thirriot, A., Charelli, F., e Yang, D. (2020). *National Capabilities Assessment Framework*. LU: European Network and Information Security Agency (ENISA). https://data.europa.eu/doi/10.2824/590072

Snyder, D., Mayer, L. A., Weichenberg, G., Tarraf, D. C., Fox, B., Hura, M., Suzanne, G., e Welburn, J. W. (2020). *Measuring Cybersecurit and Cyber Resiliency*. Santa Monica, CA: RAND Corporation.

SPMS. (2016). *Estratégia Nacional para o Ecossistema de Informação de Saúde (ENESIS) 2020*. SPMS, EPE - Serviços Partilhados do Ministério da Saúde. https://enesis.spms.min-saude.pt/wp-content/uploads/2017/07/brochura-online_v1.pdf (consultado em 30/10/2021)

UE. (2012). Special Eurobarometer 390: Cyber security. Comissão Europeia/Directorate-General for Communication. https://europa.eu/eurobarometer/surveys/detail/1058 (consultado em 30/10/2021)

UE. (2013). Special Eurobarometer 404: Cyber security. Comissão Europeia/Directorate-General for Communication. https://europa.eu/eurobarometer/surveys/detail/1073 (consultado em 30/10/2021)

UE. (2015a). Special Eurobarometer 423: Cyber security. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2019 (consultado em 30/10/2021)

UE. (2015b). Special Eurobarometer 432: Europeans' attitudes towards security. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2085 (consultado em 30/10/2021)

UE. (2017a). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2171 (consultado em 30/10/2021)

UE. (2017b). Special Eurobarometer 464b: Europeans' attitudes towards security. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/1569 (consultado em 30/10/2021)

UE. (2018). Flash Eurobarometer 464: Fake News and Disinformation Online. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2183 (consultado em 30/10/2021)

UE. (2019). Special Eurobarometer 480: Europeans' attitudes towards Internet security. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2207 (consultado em 30/10/2021)

UE. (2020). Special Eurobarometer 499: Europeans' attitudes towards cybersecurity. Comissão Europeia/Directorate-General for Communication.
https://europa.eu/eurobarometer/surveys/detail/2249 (consultado em 30/10/2021)

UE. (2021a). EU Vocabularies: Estratégia da UE. Publications Office of the European Union. https://op.europa.eu/s/u3OQ (consultado em 30/10/2021)

UE. (2021b). EU Vocabularies: Política Pública. Publications Office of the European Union. https://op.europa.eu/s/u3OS (consultado em 30/10/2021)

Wall, M. (2015). Citizen journalism: A retrospective on what we know, an agenda for what we don't. *Digital Journalism*, *3*(6), 797–813.

Walton, S., Wheeler, P. R., Zhang, Y. (Ian), e Zhao, X. (Ray). (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *Journal of Information Systems*, *35*(1), 155–186. https://doi.org/10.2308/ISYS-19-033

White, G. B. (2011). The community cyber security maturity model. In *2011 IEEE international conference on technologies for homeland security (HST)* (pp. 173–178). IEEE.

Wlezien, C., e Soroka, S. N. (2016). Public Opinion and Public Policy. In *Oxford Research Encyclopedia of Politics*. Oxford University Press.
https://doi.org/10.1093/acrefore/9780190228637.013.74

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Observatório
de Cibersegurança

CENTRO NACIONAL DE CIBERSEGURANÇA
RUA DA JUNQUEIRA, 69 | 1300-342 LISBOA
CNCS@CNCS.GOV.PT
(+351) 210 497 400