RESOLUÇÃO DO CONSELHO DE MINISTROS N.º 92/2019, DE 5 DE JUNHO - ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Resolução do Conselho de Ministros N.º 92/2019, de 5 de Junho - Estratégia Nacional de Segurança do Ciberespaço 2019-2023

Em linha com os esforços de harmonização que têm sido empreendidos na União Europeia em matéria de cibersegurança, Portugal reviu a sua Estratégia Nacional de Segurança do Ciberespaço, aprovando as grandes linhas politico-legislativas que irão orientar o país para os próximos anos. Apesar de traduzir um aprimoramento em relação à sua antecedente, a estratégia ora aprovada suscita relevantes questões jurídicas em relação à sua execução e à proteção dos direitos constitucionalmente protegidos dos cidadãos.

Council of Ministers Resolution 92/2019 of 5 June - National Strategy for the Security of Cyberspace 2019-2023

Portugal has revised its National Cybersecurity Strategy, which includes the main political and legislative guidelines for the following years, in line with the cybersecurity harmonisation efforts that are being deployed in the European Union. The strategy reflects an improvement in relation to its predecessor. Nonetheless, it prompts significant legal questions concerning its execution and the protection of citizens' constitutional rights.

Palabras clave

Segurança nacional; Cibersegurança; Defesa nacional; Cibercrime; Computadores; Redes; Direito das Tecnologias da Informação.

Key words

National security; Cybersecurity; National defence; Cybercrime; Computers; Networks; IT Law.

Fecha de recepción: 3-9-2019 *Fecha de aceptación: 4-9-2019*

1 · INTRODUÇÃO

No passado dia 5 de junho de 2019, foi publicada a Resolução do Conselho de Ministros n.º 92/2019, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 ("ENSC 2019"). O instrumento define o enquadramento, os objetivos e as linhas de ação do Estado no âmbito da cibersegurança, sendo essencial para o desenvolvimento dos mecanismos e estruturas adequados a dotar Portugal da necessária resiliência a ameaças do ciberespaço.

A presente ENSC 2019 substitui a anterior estratégia aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, sendo o segundo instrumento do tipo. As alterações legislativas e institucionais ocorridas entre a aprovação da primeira estratégia e da ENSC 2019 foram significativas, permitindo que o segundo instrumento se apoie nas estruturas entretanto criadas e convoque a operacionalização dos meios e mecanismo apropriados às finalidades prosseguidas: «*aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas*».

2 · ANTECEDENTES

A primeira versão da ENSC 2019, aprovada em 12 de junho de 2015 através da Resolução do Conselho de Ministros n.º 36/2015, constituiu um dos primeiros instrumentos político-legislativos consolidados em Portugal tendentes à adoção de uma estrutura nacional de proteção do ciberespaço.

Passados dois anos da sua aprovação, foi criado o Conselho Superior de Segurança do Ciberespaço ("CSSC"), através da Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto de 2017. Ao mesmo foi atribuída a missão de assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço e sua revisão.

Em 2018, foi aprovada a Lei n.º 46/2018, de 13 de agosto, a qual estabelece o regime jurídico da segurança do ciberespaço. Através da aprovação desta lei, foi transposta a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

A aprovação deste regime veio introduzir relevantes alterações no enquadramento legal e institucional da cibersegurança nacional. Destaca-se a atribuição

Casqueiro, Filipe de Oliveira; Casanova, Nuno Salazar: "Resolução do Conselho de Ministros N.º 92/2019, de 5 de Junho - Estratégia Nacional de Segurança do Ciberespaço 2019-2023", *Actualidad Jurídica Uría Menéndez*, 52, 2019, pp. 152-157 (ISSN: 1578-956X).

de natureza consultiva ao CSSC, o qual passa a dever ser consultado pelo Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço (onde se inclui a Estratégia Nacional da Segurança do Ciberespaço).

Também através da Lei n.º 46/2018, de 13 de agosto, designou-se o Centro Nacional de Cibersegurança ("CNCS") como Autoridade Nacional de Cibersegurança. Funcionando no âmbito do Gabinete Nacional de Segurança desde 2014, o CNCS «*tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais*».

Dentro das suas atribuições, o CNCS possui competências de regulação, regulamentação, supervisão, fiscalização e sancionatórias. Pode emitir instruções de cibersegurança e definir o nível de alerta de cibersegurança nacional. É ainda o ponto de contacto único nacional para efeitos de cooperação internacional, devendo atuar em articulação com as estruturas nacionais de responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo.

Integrado no CNSC, o serviço "CERT.PT" coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de Infraestruturas Críticas nacionais e prestadores de serviços digitais. O CERT.PT é membro da rede nacional de Equipas de Resposta a Incidentes de Segurança Informática ("*CSIRT - Computer Security Incident Response Team*") e representante nacional na Rede Europeia de CSIRT, estabelecida pela Diretiva (EU) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 (cfr. artigos 8.º e 9.º da Lei n.º 46/2018, de 13 de agosto).

A estratégia aprovada em 2015 previa a sua revisão num prazo máximo de três anos, o que veio a suceder através da aprovação da presente ENSC 2019, publicada em 5 de junho de 2019.

3 · A ENSC 2019

A ENSC 2019 recupera alguns conceitos da sua primeira versão de 2015, contendo, no entanto, aspetos inovadores em relação à sua antecedente.

Um desses aspetos é a previsão de algumas definições consideradas relevantes para a «*constituição de uma base conceptual que possa ser utilizada por todos*». Concretamente, procura-se definir quatro conceitos – "*ciberespaço*", "*cibersegurança*", "*ciberdefesa*" e "*cibercrime*", sendo clara a preocupação do legislador com a criação de uma linguagem comum às diversas entidades participantes da estratégia.

Não obstante as boas intenções do legislador, a verdade é que a (curta) lista de definições peca pela generalidade e indeterminação, pouco contribuindo para o almejado objetivo. Com efeito, a definição dos referidos conceitos é composta, por sua vez, por outros conceitos indeterminados cuja definição não é sequer unívoca na doutrina, e por terminologia técnica. É o caso paradigmático da definição de ciberespaço, que segundo a lei é «*o ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação*».

Assim, a escolha e definição pelo legislador dos referidos quatro conceitos suscita mais perguntas do que respostas, devendo ser encaradas como uma base de trabalho doutrinário, ao invés de verdadeiras definições legais.

Dos parágrafos introdutórios da ENSC 2019 destaca-se, ainda, a menção aos instrumentos internacionais a que Portugal se encontra vinculado. Em particular, é feita uma menção expressa à política de ciberdefesa da Organização do Tratado do Atlântico Norte, fruto provavelmente das iniciativas que esta organização tem adotado nos últimos anos em relação ao ciberespaço (como é o caso da declaração deste como domínio de operações, cfr. Declaração de Varsóvia de 9 de Julho de 2016[1]).

A fechar a parte introdutória da ENSC 2019, estabelecem-se três princípios estruturais: *subsidiariedade*, *complementaridade* e *proporcionalidade*. A enunciação destes três princípios tem repercussões não só na política legislativa, mas também na interpretação jurídica das normas e medidas administrati-

1 Acessível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm

vas que venham a ser adotados no âmbito da presente estratégia. Curiosamente, a ENSC 2019 deixou cair os princípios da cooperação e sensibilização previstos na estratégia de 2015, relegando-se essas matérias para os eixos de atuação que se mencionarão *infra*.

3.1 · Princípio da subsidiariedade

Na ENSC 2019, é reconhecido que grande parte das infraestruturas tecnológicas é detida por entidades privadas, sendo estas quem as controla do ponto de vista jurídico e operacional. Com base nesta premissa, a ENSC 2019 direciona a responsabilidade pela cibersegurança das infraestruturas para os respetivos privados (incluindo os próprios indivíduos), apresentando-se o Estado como última linha da segurança do ciberespaço e como garante da soberania e dos princípios constitucionais.

Pela forma como se encontra descrito, o princípio aparenta ter sido pensado para delimitar a atuação do Estado nas infraestruturas detidas por privados. Porém, não deverá ser esquecido que o próprio Estado controla e detém importantes serviços públicos situados no ciberespaço, onde se inclui parte da defesa nacional. Tais serviços requerem, desde logo, uma responsabilização direta do próprio Estado na manutenção da sua segurança.

Em face desta constatação, e considerando a abrangência do presente instrumento, estranha-se que o «*forte compromisso*» de Portugal com a segurança do ciberespaço se encontre previsto sob o princípio da subsidiariedade, e não se tenha aproveitado a oportunidade para afirmar cristalinamente o princípio da responsabilidade direta do Estado na segurança e defesa do ciberespaço.

Até porque, na estratégia de 2015, o Estado declarava claramente que, a propósito do princípio da subsidiariedade, «*a segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço*»[2].

Em suma, o princípio da subsidiariedade enunciado na ENSC 2019 deverá ser considerado na regulação das relações entre Estado e particulares no âmbito da cibersegurança. No entanto, é manifesto que o princípio da subsidiariedade não prejudica o princípio da responsabilidade do Estado pelas estruturas por si direta ou indiretamente controladas, o qual deverá pautar as medidas a serem adotadas no âmbito da presente estratégia.

3.2 · Princípio da complementaridade

Na ENSC 2019, enuncia-se que a interdependência das infraestruturas tecnológicas, independentemente das entidades titulares ou controladoras, poderá gerar incidentes com efeitos sistémicos. Desses incidentes, poderá resultar a indisponibilidade e violação da integridade dos dados e das estruturas (incluindo eventuais quebras de confidencialidade).

Em face desta constatação, é enunciado o princípio da responsabilidade partilhada entre atores públicos e privados, impondo-se um dever de cooperação reforçada entre as entidades nacionais. A cooperação entre entidades é, aliás, profusamente repetida ao longo de toda a ENSC 2019, concretizando-se a mesma na partilha de informação e de conhecimentos.

Noutra perspetiva, pode-se afirmar que o princípio da complementaridade é o reconhecimento da incapacidade do Estado de garantir, por si só, um nível de cibersegurança nacional suficientemente elevado para defender os direitos e interesses legalmente protegidos. Como consequência, "impõe-se" a cooperação entre entidades públicas e privadas, as quais se complementarão nas funções de segurança a executar.

Porém, a anunciada complementaridade não deverá ser entendida como suplência das entidades privadas em relação às funções públicas. Com efeito, em decorrência do atrás referido princípio da responsabilidade, o Estado deverá tomar a dianteira das funções de segurança do ciberespaço: começando nos serviços públicos por si controlados e acabando na intervenção subsidiária junto das entidades privadas.

Acresce que, em contraponto às obrigações de cooperação impostas a entidades privadas, existirão outros direitos legais (propriedade privada, privacidade, propriedade intelectual, segredos comerciais, entre outros) cuja ponderação terá de ser devidamente acautelada, através da competente intervenção legislativa. Necessidade de ponderação que parece ter sido esquecida na presente

2 Declaração que aparece hoje referida apenas ao nível dos eixos de atuação.

estratégia, confiando-se que o legislador a fará aquando da sua execução.

3.3 · Principio da proporcionalidade

O último princípio previsto na ENSC 2019 relaciona os riscos identificados e a execução das linhas de atuação, impondo que a adequação e alocação dos recursos seja proporcional àqueles.

Não obstante a parca descrição contida na estratégia sobre a aplicação do princípio da proporcionalidade (focada, essencialmente, na perspetiva dos custos orçamentais), a verdade é que a aplicação do princípio da proporcionalidade tem um campo mais vasto, mais que não seja por imposição constitucional.

Com efeito, acima se referiu que a medida e extensão das obrigações de cooperação dos privados com o Estado têm de ser determinadas com ponderação dos demais direitos e interesses legais afetados. Aliás, a própria ENSC 2019 prevê a «*proteção da liberdade de expressão, dos dados pessoais e da privacidade*», acrescentando nós que outros direitos fundamentais poderão ser afetados pelas medidas legais e administrativas que venham a ser adotadas em consequência da implementação da estratégia.

Consequentemente, a lei e a própria Constituição impõem que as medidas a ser adotadas no âmbito da cibersegurança devam respeitar os princípios de adequação, necessidade e proporcionalidade, não só em relação aos custos orçamentais, mas também em relação a outros direitos e interesses legalmente protegidos.

4 · VISÃO E OBJETIVOS ESTRATÉGICOS

A ENSC 2019 procura que, em 2023, «*Portugal seja 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*». Para tanto, estabelece três objetivos estratégicos: (i) *maximizar a resiliência*; (ii) *promover a inovação*; e, (iii) *gerar e garantir recursos*.

Por forma a alcançar estes objetivos, são estabelecidos seis eixos de atuação, os quais se passarão a detalhar.

5 · EIXOS DE ATUAÇÃO

5.1 · Eixo 1 – Estrutura de segurança do ciberespaço

O primeiro eixo de atuação traduz-se na criação de uma estrutura nacional que reúna recursos, conhecimentos e competências destinados a exercer a função de segurança do ciberespaço.

Refletindo as alterações legislativas e institucionais implementadas desde a aprovação da sua primeira versão, a ENSC 2019 procura consolidar o papel do CSSC e do CNCS (incluindo o serviço "CERT.PT") como entidades de referência em matéria de cibersegurança nacional.

Não obstante a aparente centralização institucional, é mantida a difusão de atribuições em matéria de cibersegurança entre outras entidades públicas com competências especializadas. É o caso do *Ministério Público* e da *Polícia Judiciária* (cooperação internacional em matéria penal), das *Forças Armadas* (ciberdefesa), do *Secretário-Geral do Sistema de Informações* (informações de segurança nacional, externa e interna) e do *Secretário-Geral do Sistema de Segurança Interna* (Ponto Único de Contacto em matéria de cooperação policial internacional e situações de alerta e resposta rápidas às ameaças à segurança interna).

Através da ENSC 2019, Portugal declara que, no âmbito da ciberdefesa, irá dotar-se de capacidades ofensivas. Esta declaração, apesar de carecer de concretização, parece indiciar que serão investidos recursos na capacitação das Forças Armadas para ataque a alvos no ciberespaço, faltando perceber o enquadramento em que os mesmos serão executados.

Destaca-se, ainda, o estabelecimento do princípio de cooperação entre a função de ciberdefesa nacional e de segurança interna. A asserção deste princípio coloca questões juridicamente relevantes, sendo, designadamente, necessário verificar de que forma será garantida a independência no âmbito de atuação dos serviços de defesa e segurança (em particular, como será evitado o uso de recursos militares contra cidadãos nacionais).

Por fim, prevê-se o desenvolvimento de uma área especial de diplomacia – ciberdiplomacia – como forma de coordenação da ação externa do Estado, realçando-se as relações com a Comunidade dos Países de Língua Portuguesa.

5.2 · Eixo 2 - Prevenção, educação e sensibilização

No âmbito do Eixo 2, é concedida ênfase às funções de prevenção, educação e sensibilização.

Quanto à prevenção, prevê-se a partilha de informação na avaliação precoce da ameaça, estabelecendo-se a necessidade de desenvolver e difundir indicadores de ameaça, que possam ser adequados a desencadear respostas preventivas.

Em relação à educação e sensibilização, procura-se aumentar a resiliência nacional mediante a difusão de conhecimento entre entidades públicas e privadas, capacitando os utilizadores finais com formação adequada a prevenir os riscos do ciberespaço.

5.3 · Eixo 3 - Proteção do ciberespaço

No terceiro eixo de atuação, são apresentadas medidas destinadas a garantir a segurança do ciberespaço. Destaca-se o impulso dado à identificação e consolidação do conhecimento das infraestruturas críticas e à aplicação de mecanismos de segurança do ciberespaço que sejam por estas implementados.

Também se prevê a cooperação entre entidades empresariais públicas e privadas, bem como de outras entidades públicas ao nível central, regional e local. Em particular, salienta-se a necessidade de partilha de informação e de conhecimento, com vista a desenvolver a prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço. Veja-se, a propósito, o referido *supra* quanto ao princípio da complementaridade e à necessidade de ponderação de outros direitos e interesses legais no estabelecimento da extensão e limites às referidas obrigações de cooperação dos particulares.

5.4 · Eixo 4 - Resposta às ameaças e combate ao cibercrime

No quarto eixo de atuação, a ENSC 2019 começa por salientar a relevância da cooperação entre entidades que, por força das suas atribuições, detenham informação relevante para efeitos de prevenção e resposta a ameaças no ciberespaço. Dessa cooperação, espera-se a conjugação de sinergias que permitam a atribuição de autoria (*accountability*) ou que auxiliem as investigações em curso.

É, ainda, referida a necessidade de desenvolvimento de mecanismos de dissuasão, de meios de identificação e de resposta à ameaça. A propósito desta declaração, e considerando a dinâmica própria e assimétrica que os ataques cibernéticos tendencialmente possuem, permanece a questão de saber se, em âmbito de segurança nacional, serão desenvolvidas capacidades ofensivas de disrupção como forma de coação policial e de que forma serão garantidos e respeitados os direitos fundamentais dos cidadãos.

Tal como referido no Eixo 1, também neste eixo se prevê a adoção de medidas que permitam uma abordagem integrada às ameaças pelas Forças Armadas e Forças de Segurança. Esta constatação apenas reforça a preocupação do uso de capacidades militares, ainda que de forma indireta, contra ameaças unicamente nacionais ou de âmbito meramente criminal.

Por fim, a ENSC 2019 refere expressamente a agilização de ações de investigação online, incluindo as que possam enquadrar-se no contexto de ações encobertas. A previsão e delimitação do uso de ações encobertas no âmbito da cibersegurança nacional é juridicamente melindrosa, podendo resultar na violação de direitos fundamentais dos cidadãos. Além de que o seu conhecimento pelo público em geral poderá contribuir, desde logo, para a redução de confiança no uso do ciberespaço pelos cidadãos, na medida em que a difusão da ação policial dissimulada se converta numa devassa da privacidade. Acresce que a atuação policial encoberta poderá adquirir, do ponto de vista operacional, características semelhantes a um ataque cibernético, o que legitimará o uso de mecanismos defensivos pelos cidadãos, em linha com as suas próprias políticas de cibersegurança, frustrando-se, assim, as finalidades da atuação policial.

5.5 · Eixo 5 - Investigação, desenvolvimento e inovação

Intimamente ligado ao Eixo 2, o Eixo 5 visa o desenvolvimento de conhecimento e tecnologias inovadores, que possam ser aplicados pelos diversos atores públicos e privados no âmbito da cibersegurança.

Destaca-se a referência à participação em trabalhos de comissões técnicas nacionais e internacionais, para implementar normas e especificações técnicas internacionalmente aceites aplicáveis à segurança

das redes e dos sistemas de informação. Prevê-se, no entanto, que não haverá imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, em linha com o art. 12.º da Lei n.º 46/2018, de 13 de agosto.

5.6 · Eixo 6 – Cooperação nacional e internacional

O último eixo de atuação vem destacar uma ideia transversal a todos os eixos: o dever de cooperação entre entidades públicas e privada em matéria de cibersegurança. No que concerne às entidades com responsabilidade nas áreas que contribuem para a segurança do ciberespaço, prevê-se que esse dever de cooperação seja reforçado.

A cooperação internacional é também salientada, frisando-se a participação de Portugal «*nos órgãos, organismos e agências relevantes, nomeadamente, da Organização das Nações Unidas, da União Europeia, da Organização do Tratado do Atlântico Norte*» e da «*Organização para a Segurança e Cooperação na Europa*».

As medidas de coordenação e cooperação previstas neste eixo visam não só a partilha de informação e conhecimento de boas práticas, como também a capacidade de alerta e resposta às ameaças de cibersegurança.

6 · CONSIDERAÇÕES FINAIS

A ENSC 2019 reflete um aprimoramento da estratégia nacional em matéria de cibersegurança, conjugando as estruturas entretanto criadas desde a sua primeira aprovação. Sendo um instrumento por natureza genérico, demonstra, contudo, o alinhamento de Portugal com os esforços que têm sido empreendidos em matéria de cibersegurança por diversos Estados estrangeiros.

Decorrente da breve análise que ora se efetuou, destacam-se três reservas à presente ENSC 2019:

Em primeiro lugar, denota-se a existência de múltiplas entidades nacionais com atribuições em matéria de cibersegurança.

Se, por um lado, a transversalidade do uso do ciberespaço determina o contacto com diversas áreas de atuação; por outro, antevê-se que multiplicação de entidades administrativas com intervenção em áreas sobrepostas às de outras coloque uma pressão extraordinária na coordenação entre aquelas. Em consequência, caso a coordenação seja insuficiente, poderá ficar em causa o cumprimento dos fins prosseguidos pelas diversas entidades, bem como poderão surgir respostas díspares que comprometam os direitos dos particulares.

Em segundo lugar, realça-se que, ao longo ENSC 2019, são previstos objetivos e medidas do âmbito civil e militar, chegando-se a afirmar a necessidade de abordagens integradas.

Não obstante a estratégia carecer de concretização legislativa e regulamentar, revela-se desde já preocupante a possibilidade da anunciada "cooperação" e "troca de informação", entre entidades de segurança interna e forças armadas, acarretar a utilização de recursos militares contra cidadãos (ainda que de forma indireta).

Em terceiro lugar, apesar da cooperação e partilha de informação entre o Estado e entidades privadas ser uma pedra angular da presente estratégia, pouco se investiu na definição dos limites e dos critérios de ponderação entre as obrigações de cooperação e outros direitos e interesses legalmente previstos. Caso essa ponderação não venha a ser convenientemente realizada, através das medidas legislativas e regulamentares adequadas, poderá verificar-se um aumento dos litígios entre particulares e o Estado.

Finalmente, tal como a sua antecessora, a ENSC 2019 deverá ser revista, pelo menos, no prazo de cinco anos, competindo ao CSSC avaliar anualmente a adequação dos objetivos estratégicos e do plano de ação.

Filipe de Oliveira Casqueiro y Nuno Salazar Casanova (*)

(*) Abogados del Área de Derecho Público, Procesal y Arbitraje de Uría Menéndez (Lisboa).