ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

EXCELENTÍSSIMO SENHOR
PRESIDENTE DA ASSEMBLEIA DA REPUBLICA

Ofício n.º 479/XIII/1ª – CACDLG/2018 **Data: 9-05-2018**

NU: 601026

ASSUNTO: Parecer sobre a Proposta de Lei n.º 119/XIII/3.ª (GOV).

Para os devidos efeitos, junto se envia o parecer relativo à Proposta de Lei n.º 119/XIII/3.ª (GOV) - Estabelece o regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148, tendo as respetivas partes I e III sido aprovadas por unanimidade, verificando-se a ausência do PEV, na reunião de 9 de maio de 2018 da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias.

Com os melhores cumprimentos,

O PRESIDENTE DA COMISSÃO

(Bacelar de Vasconcelos)

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias
Assembleia da República – Palácio de São Bento - 1249-068 Lisboa
Tel. 21 391 92 91/96 67 / Fax: 21 393 69 41 / E-mail: 1CACDLG@ar.parlamento.pt

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

PARECER

PROPOSTA DE LEI N.º 119/XIII/3.ª – Estabelece o regime jurídico da segurança no ciberespaço, transpondo a Diretiva (UE) 2016/1148

PARTE I - CONSIDERANDOS

I. a) Nota introdutória

O Governo aprovou, em 15 de março de 2018, a Proposta de Lei n.º 119/XIII/3.ª – "Estabelece o regime jurídico da segurança no ciberespaço, transpondo a Diretiva (UE) 2016/1148".

Esta Proposta foi apresentada à Assembleia da República nos termos do disposto na alínea d) do n.º 1 do artigo 197.º da Constituição da República Portuguesa e do artigo 118.º do Regimento da Assembleia da República, reunindo os requisitos formais previstos no artigo 124.º desse mesmo Regimento.

Tendo dado entrada na Assembleia da República em 26 de março de 2018, a Proposta baixou à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias para emissão do respetivo parecer, por despacho de Sua Excelência o Presidente da Assembleia da República datado de 28 de março de 2018.

I b) Objetivos da proposta do Governo

A Proposta de Lei n.º 119/XIII/3.ª, apresentada pelo Governo, estabelece o regime jurídico da segurança no ciberespaço, transpondo para a ordem jurídica nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, que define as medidas destinadas a garantir um nível comum elevado de segurança das redes e dos sistemas de informação em toda a União Europeia. Deve notar-se que o artigo 25.º n.º 1 da Diretiva fixa a data de 9 de maio como limite para a transposição que justifica esta Proposta de Lei.

A referida Diretiva estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e sistemas de informação, identifica um conjunto de requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais e faz impender sobre os Estados-Membros a obrigação de designarem as autoridades nacionais responsáveis, os pontos de contacto únicos nacionais e as equipas de resposta a incidentes de segurança informática nacionais.

A Proposta de Lei enquadra a missão de transposição desta Diretiva para o direito português considerando que "a abrangência, frequência e impacto dos incidentes de segurança estão a aumentar", o que "pode colocar em causa o regular funcionamento da sociedade, acarretar perigo para a vida humana, perdas de natureza financeira, bem como comprometer a confidencialidade, a integridade e a disponibilidade da informação das redes e dos sistemas de informação da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais".

I c) Descrição sumária dos conteúdos da Proposta de Lei

Em vista do objetivo acima referido, a Proposta de Lei em apreço prevê a aprovação de uma Estratégia Nacional de Segurança do Ciberespaço; a estrutura

nacional de segurança do ciberespaço; a identificação dos operadores de serviços essenciais pelo Centro Nacional de Cibersegurança; o ponto de contacto único nacional para efeitos de cooperação internacional; requisitos de segurança nas redes e sistemas de informação e obrigações de notificação de incidentes ao Centro Nacional de Cibersegurança; e o quadro contraordenacional aplicável a violações da lei.

De acordo com o artigo 2.º n.º 1, a lei proposta aplicar-se-á à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a quaisquer outras entidades que utilizem redes e sistemas de informação. O n.º 6 do mesmo artigo estatui que a lei não se aplica nem às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas nem às redes e sistemas de informação que processem informação classificada. Estas redes e sistemas de informação ficam, pois, sujeitas a regime específico.

Na economia deste diploma, a Estratégia Nacional de Segurança do Ciberespaço surge em primeiro lugar (artigo 4.º), como devendo ser aprovada por Resolução do Conselho de Ministros, sob proposta do Primeiro-Ministro, ouvido o Conselho Superior de Segurança do Ciberespaço. Refira-se que a Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, aprovou a primeira versão da Estratégia Nacional de Segurança do Ciberespaço com quatro objetivos principais: a) promoção de uma utilização consciente, livre, segura e eficiente do ciberespaço; b) proteção dos direitos fundamentais, da liberdade de expressão, dos dados pessoais e da privacidade dos cidadãos; c) fortalecimento e garantia da segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e d) afirmação do ciberespaço como domínio de desenvolvimento económico e de inovação.

A estrutura de segurança do ciberespaço inclui um Conselho Superior de Segurança do Ciberespaço (artigos 5.º e 6.º), um Centro Nacional de Cibersegurança (artigo 7.º) que é a autoridade nacional de cibersegurança, e uma

equipa de resposta a incidentes de segurança informática nacional (CERT.PT) (artigos 8.º e 9.º).

Os artigos 12.º e seguintes da Proposta definem os requisitos de segurança das redes e dos sistemas de informação. A saber: requisitos de segurança e normalização (artigo 12.º), requisitos de notificação de incidentes (artigo 13.º), requisitos de segurança para a Administração Pública e operadores de infraestruturas críticas (artigo 14.º), para os operadores de serviços essenciais (artigo 16.º) e para os prestadores de serviços digitais (artigo 18.º). Nos artigos 15.º, 17.º e 19.º fixam-se os contornos das obrigações de notificação de incidentes a cargo respetivamente da Administração Pública e operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais.

Finalmente, os artigos 21.º e seguintes regulam o regime contraordenacional aplicável a violações da lei agora proposta. As contraordenações são divididas em graves (artigo 24.º) e muito graves (artigo 23.º). De notar que o valor das coimas estabelecido nestes dois artigos é considerado pela Comissão Nacional de Proteção de Dados, no seu parecer, como "irrisório".

I d) Opinião do Deputado Relator

Nos termos do n.º 3 do artigo 137.º do Regimento da Assembleia da República, o signatário do presente relatório entende, neste parecer, não manifestar a sua opinião política pessoal sobre a Proposta de Lei n.º 119/XIII/3.ª, reservando-a para a respetiva discussão em sessão plenária.

PARTE II – CONCLUSÕES

1. O Governo aprovou, em 15 de março de 2018, a Proposta de Lei n.º 120/XIII/3.ª – "Estabelece o regime jurídico da segurança no ciberespaço, transpondo a Diretiva (UE) 2016/1148".
2. A Proposta de Lei em apreço estabelece o regime jurídico da segurança no ciberespaço, transpondo para a ordem jurídica nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, que define as medidas destinadas a garantir um nível comum elevado de segurança das redes e dos sistemas de informação em toda a União Europeia.
3. Tendo em conta o exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias é de parecer que a Proposta de Lei n.º 119/XIII/3.ª reúne os requisitos constitucionais e regimentais para ser discutida e votada em plenário.

Palácio de S. Bento, 9 de maio de 2018

O Deputado Relator	**O Presidente da Comissão**
(José Manuel Pureza)	***(Pedro Bacelar de Vasconcelos)***

Anexo: Anexa-se a Nota Técnica elaborada pelos serviços de apoio à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, ao abrigo do disposto no artigo 131.º do Regimento da Assembleia da República.

Nota Técnica

Proposta de Lei n.º 119/XIII/3.ª (Governo)

Estabelece o regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148

Data de admissão: 28 de março de 2018

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª)

Índice

I. Análise sucinta dos factos, situações e realidades respeitantes à iniciativa

II. Apreciação da conformidade dos requisitos formais, constitucionais e regimentais e do cumprimento da lei formulário

III. Enquadramento legal e doutrinário e antecedentes

IV. Iniciativas legislativas e petições pendentes sobre a mesma matéria

V. Consultas e contributos

VI. Apreciação das consequências da aprovação e dos previsíveis encargos com a sua aplicação

Elaborada por: Ana Vargas (DAPLEN), Catarina R. Lopes e Cláudia Sequeira (DAC), Paula Faria (BIB) e Cristina Ferreira (DILP)

Data: 16 de abril de 2018

I. Análise sucinta dos factos, situações e realidades respeitantes à iniciativa

Com a Proposta de Lei *sub judice*, o Governo propõe o regime jurídico da segurança do ciberespaço, transpondo[1] 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.

Sublinhamos que a iniciativa define redes e sistemas de informação como "*qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção*"[2].

Segundo a respetiva exposição de motivos, as "*redes e os sistemas de informação desempenham um papel vital na sociedade, sendo a sua resiliência e segurança essenciais para a prossecução de atividades económicas e societais.*"

Quanto ao âmbito, esta Proposta de Lei é aplicável:

- à Administração Pública[3];
- aos operadores de infraestruturas críticas;
- aos operadores de serviços essenciais;
- aos prestadores de serviços digitais[4]; e
- a quaisquer entidades que utilizem redes e sistemas de informação.

[1] De acordo com o n.º 1 do artigo 25.º da referida Diretiva, o prazo para a transposição acaba a 9 de maio de 2018.
[2] Segundo a alínea k) do artigo 3.º.
[3] Incluí: o Estado; as regiões autónomas; as autarquias locais; as entidades administrativas independentes; os institutos públicos; as empresas públicas e as associações públicas.
[4] Desde que tenham o seu estabelecimento principal em Portugal, ou tenham um representante estabelecido e prestem serviços digitais em Portugal.

Ficam fora do seu âmbito as redes e sistemas de informação: diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas; e que processem informação classificada.

Esta Proposta de Lei prevê:

- a aprovação de uma Estratégia Nacional de Segurança do Ciberespaço[5];
- a estrutura nacional de segurança do ciberespaço[6];
- a identificação dos operadores de serviços essenciais pelo Centro Nacional de Cibersegurança;
- o ponto de contacto único nacional para efeitos de cooperação internacional;
- que algumas entidades tenham de observar determinados requisitos de segurança nas suas redes e sistemas de informação, bem como de notificar eventuais incidentes[7] ao Centro Nacional de Cibersegurança;
- a possibilidade de notificação voluntária de incidentes por parte das entidades não abrangidas pela obrigação legal;
- o quadro contraordenacional estabelecendo infrações graves e muito graves.

A definição dos requisitos de segurança e de notificação de incidentes são remetidos para regulamentação posterior.

A Proposta de Lei em apreço compõe-se de cinco capítulos, num total de 33 artigos, e um Anexo: Capítulo I – Disposições Gerais (artigos 1.º a 4.º); Capítulo II – Estrutura de segurança do ciberespaço (artigos 5.º a 11.º); Capítulo III – Segurança das redes e dos sistemas de informação (artigos 12.º a 20.º); Capítulo IV – Fiscalização e sanções (artigos 21.º a 28.º); Capítulo V – Disposições finais (artigos 29.º a 33.º).

A Proposta de Lei determina o seu início de vigência para o dia seguinte ao da sua publicação, com exceção do regime decorrente dos artigos 14.º a 27.º que produz efeitos seis meses após a entrada em vigor da iniciativa.

[5] A Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, que aprovou a Estratégia Nacional de Segurança do Ciberespaço, impôs a revisão da mesma num prazo máximo de três anos.
[6] Compreendendo: o Conselho Superior de Segurança do Ciberespaço, o Centro Nacional de Cibersegurança (Autoridade Nacional de Cibersegurança), o "CERT.PT" (equipa de resposta a incidentes de segurança informática nacional, funcionando no Centro Nacional de Cibersegurança), os operadores de serviços essenciais e os prestadores de serviços digitais.
[7] Cf. a alínea c) do artigo 3.º da iniciativa em pareço define-se incidente como um evento que tem um efeito adverso real na segurança das redes e dos sistemas de informação.

Acresce que a proposta pode ainda vir a ser aperfeiçoada na fase de discussão e votação na especialidade[8].

II. Apreciação da conformidade dos requisitos formais, constitucionais e regimentais e do cumprimento da lei formulário

- **Conformidade com os requisitos formais, constitucionais e regimentais**

A Proposta de Lei n.º 119/XIII foi apresentada pelo Governo, no âmbito do seu poder de iniciativa, previsto no n.º 1 do artigo 167.º e na alínea d) do n.º 1 do artigo 197.º da Constituição, e no artigo 118.º do Regimento da Assembleia da República (RAR).

A iniciativa toma a forma de proposta de lei, nos termos do n.º 1 do artigo 119.º do RAR, encontra-se redigida sob a forma de artigos, tem uma designação que traduz sinteticamente o seu objeto principal e é precedida de uma breve exposição de motivos, mostrando-se, assim, conforme com o disposto nas alíneas a), b) e c) do n.º 1 do artigo 124.º do RAR. De igual modo, observa os requisitos formais relativos às propostas de lei, constantes das alíneas a), b) e c) do n.º 2 do artigo 124.º do RAR.

Nos termos do n.º 3 do artigo 124.º do Regimento, as propostas de lei devem ser acompanhadas dos estudos, documentos e pareceres que as tenham fundamentado, o que não acontece no caso vertente, desconhecendo-se se existem ou não documentos desse cariz no âmbito da iniciativa.

A presente iniciativa respeita os limites à admissão da iniciativa, previstos no n.º 1 do artigo 120.º do RAR, uma vez que não parece infringir a Constituição ou os princípios nela consignados e define concretamente o sentido das modificações a introduzir na ordem jurídica.

A proposta de lei deu entrada a 26 de março de 2018, tendo sido admitida e anunciada no dia 28 de março, data em que baixou, por despacho de S. Ex.ª o Presidente da Assembleia da República, à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª).

- **Verificação do cumprimento da lei formulário**

[8] Nos n.º 4 do artigo 18.º, n.º 9 do artigo 19.º e n.º 2 do artigo 30.º onde se lê "Decreto-Lei n.º 372/2007, de 6 de junho" deve-se ler "Decreto-Lei n.º 372/2007, de 6 de novembro". Não há uniformidade quanto à referência em € dos valores das coimas, no n.º 2, do artigo 24.º e no n.º 2 do artigo 23.º

A Lei n.º 74/98, de 11 de novembro, alterada e republicada pela Lei n.º 43/2014, de 11 de julho, doravante designada como lei formulário, contém um conjunto de normas sobre a publicação, identificação e formulário dos diplomas que são relevantes em caso de aprovação da presente iniciativa e que, por isso, deverão ser tidas em conta no decurso do processo da especialidade na Comissão e, em particular, aquando da redação final.

Assim, desde logo cumpre referir que a iniciativa *sub judice* contém uma exposição de motivos e obedece ao formulário das propostas de lei, em conformidade com o disposto no artigo 13.º da lei formulário e no n.º 2 do artigo 123.º do RAR, apresentando sucessivamente, após o articulado, a data de aprovação em Conselho de Ministros, em 15 de março de 2018, e as assinaturas do Primeiro-Ministro, da Ministra da Presidência e da Modernização Administrativa e do Secretário de Estado dos Assuntos Parlamentares.

A proposta de lei que "Estabelece o regime jurídico da segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148", tem um título que traduz sinteticamente o seu objeto, de acordo com o disposto n.º 2 do artigo 7.º, e indica que procede a uma transposição de Diretiva em conformidade com o n.º 4 do artigo 9.º ambos da lei formulário. Pode, no entanto, ser aperfeiçoado, nomeadamente para aproximação ao objeto. Assim, em caso de aprovação, sugere-se a seguinte alteração ao título:

"Regime jurídico da segurança do Ciberespaço (transpõe 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 da informação em toda a União)"

Por fim, assinala-se que, em caso de aprovação, a iniciativa em apreço, revestindo a forma de lei, será objeto de publicação na 1.ª série do *Diário da República*, nos termos da alínea c) do n.º 2 do artigo 3.º da lei formulário. No que diz respeito à entrada em vigor, mostrando-se em conformidade com o disposto no n.º 1 do artigo 2.º da lei formulário, o artigo 5.º da proposta de lei determina que aquela ocorra no dia seguinte ao da sua publicação, com exceção do regime decorrente dos artigos 14.º a 27.º que produz efeitos seis meses após a entrada em vigor. Refira-se, contudo que, em sede de especialidade se deverá apreciar esta disposição, pois as referidas normas abrangem matérias distintas, desde os requisitos de segurança para a administração pública e operadores de infraestruturas críticas, às disposições relativas à fiscalização e sanções, não se tratando de um regime apenas.

Refira-se ainda que, como será em seguida detalhado, revoga a Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto.

Na presente fase do processo legislativo a iniciativa em apreço não nos parece suscitar outras questões em face da lei formulário.

III. Enquadramento legal e doutrinário e antecedentes

- **Enquadramento legal nacional e antecedentes**

A iniciativa, que vem transpor a Diretiva (UE) n. º 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 da informação em toda a União.

A utilização da informática está prevista, desde 1976, no artigo 35.º da Constituição da República Portuguesa (CRP) que estabelece a proibição de uso da informática para tratamento de dados de cariz privado, *e.g.* convicções políticas, religiosas, tendo, com a revisão de 1982, sido adicionadas as convicções filosóficas, a filiação partidária ou sindical e, com a revisão constitucional de 1997, a origem étnica.[9]

A estrutura de segurança do ciberespaço é composta pelo Conselho Superior de Segurança do Ciberespaço (CSSC), pelo Centro Nacional de Cibersegurança (CNCS), investido da qualidade de Autoridade Nacional de Cibersegurança, e pela equipa de resposta a incidentes de segurança informática nacional – o CERT.PT – a funcionar no Centro Nacional de Cibersegurança. Prevê-se que o CSSC tenha um papel ativo na definição, acompanhamento e revisão da Estratégia Nacional de Segurança do Ciberespaço e que o CNCS funcione como coordenador operacional e de autoridade nacional em matéria de cibersegurança.

O CSSC foi constituído como um grupo de projeto pela Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto, que é agora revogada pela presente proposta de lei. O Despacho n.º

[9] O artigo 35.º foi alterado em 1982, pelo artigo 27.º da Lei Constitucional n.º 1/82, de 30 de setembro, em 1989, pelo artigo 20.º da Lei Constitucional n.º 1/89, de 8 de julho, e em 1997 pelo artigo 18.º da Lei Constitucional n.º 1/97, de 20 de setembro. As diversas versões do artigo 35.º podem ser consultadas aqui.

1195/2018,de 20 de dezembro de 2017, publicado no Diário da República (DR) II Série, n.º 24, de 2 de fevereiro de 2018, aprova o seu regulamento interno.

A aprovação da Estratégia Nacional de Segurança do Ciberespaço (ENSC), pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, foi motivada pela «necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política e estratégica do país, bem como o crescente número de incidentes e ataques maliciosos,» o que impõe «que a segurança do ciberespaço seja considerada uma prioridade nacional». A Estratégia estabelece os «objetivos e as linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional (…)». Os seus objetivos estratégicos consistem na promoção de uma utilização consciente, livre, segura e eficiente do ciberespaço; na proteção dos direitos fundamentais, da liberdade de expressão, dos dados pessoais e da privacidade dos cidadãos; no fortalecimento e garantia da segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e, na afirmação do ciberespaço como domínio de desenvolvimento económico e de inovação. A sua implementação assenta nos seguintes seis eixos de intervenção: a estrutura de segurança do ciberespaço (Eixo 1); o combate ao cibercrime (Eixo 2); a proteção do ciberespaço e das infraestruturas (Eixo 3); a educação, sensibilização e prevenção (Eixo 4); a investigação e desenvolvimento (Eixo 5); e, a cooperação (Eixo 6).
Conforme previsto na própria Resolução que a criou, a Estratégia deverá ser revista no decurso do presente ano.

O funcionamento do Conselho Nacional de Cibersegurança foi instituído, no âmbito do Gabinete Nacional de Segurança, pelo Decreto-Lei n.º 69/2014, de 9 de maio[10], que procedeu à segunda alteração do Decreto-Lei n.º 3/2012, de 16 de janeiro[11] («Aprova a orgânica do Gabinete Nacional de Segurança»). As competências do CNCS encontram-se previstas no artigo 2.º-A deste diploma. Na qualidade de coordenador operacional compete ao CNCS a articulação e estreita cooperação com as entidades nacionais responsáveis pela ciberdefesa, cibercrime, ciberterrorismo e ciberespionagem.

[10] Recomenda-se a leitura do Preâmbulo do Decreto-Lei n.º 69/2014, no qual se descreve os antecedentes do Centro Nacional de Cibersegurança.

[11] Alterado pelos Decretos-Leis n.º162/2013, de 4 de dezembro, n.º 69/2014, de 9 de maio, e n.º 136/2017, de 6 de novembro. Versão consolidada retirada do portal do DRE.

Importa, assim, destacar ao nível da ciberdefesa, a Orientação Política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, de 11 de outubro, publicado no DR, II Série, n.º 208, de 28 de outubro de 2013.

No âmbito do cibercrime e combate ao terrorismo, registe-se a Lei do Cibercrime aprovada pela Lei n.º 109/2009, de 15 de setembro, a Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7.º-A/2015, de 20 de fevereiro, e a Lei de Combate do Terrorismo (em cumprimento da Decisão Quadro n.º 2002/475/JAI, do Conselho, de 13 de Junho), aprovada pela Lei n.º 52/2003, de 22 de agosto, (versão consolidada) que procedeu à décima segunda alteração ao Código de Processo Penal e décima quarta alteração ao Código Penal. (Vd. trabalhos preparatórios).

Destaca-se, também, a criação na Polícia Judiciária, da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, pelo Decreto–Lei n.º 81/2016, de 28 de novembro, bem como a criação do Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade (Gabinete Cibercrime) que tem sede na Procuradoria-Geral da República, e foi criado por Despacho do Procurador-Geral da República, a 7 de dezembro de 2011.

Ao nível da segurança interna salienta-se a Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, (versão consolidada).[12] (Vd. trabalhos preparatórios).

No âmbito da missão do CNCS de contribuir para que o país use o ciberespaço de uma forma segura, confiável e livre, em particular no que diz respeito à segurança das redes e dos sistemas de informação, importa destacar a legislação essencial na área da proteção das infraestruturas essenciais, de programas de computador e de bases de dados, bem como do comércio eletrónico. Assim,

- O Decreto-Lei n.º 62/2011, de 9 de maio, que estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro;
- O Decreto-Lei n.º 252/94, de 20 de outubro[13], que transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de proteção jurídica dos programas de computador (versão consolidada);

[12] Retificada pela Declaração de Retificação n.º 66-A/2008, de 28 de outubro e alterada pela Lei n.º 59/2015, de 24 de junho e pelo Decreto-Lei n.º 49/2017, de 24 de maio.

[13] Retificado pela Declaração de Retificação n.º 2-A/95, de 31 de janeiro, e alterado pelo Decreto-Lei n.º 334/97, de 27 de novembro.

- O Decreto-Lei n.º 122/2000, de 4 de julho, transpõe para a ordem jurídica interna a Diretiva n.º 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de Março, relativa à proteção jurídica das bases de dados;
- O Decreto-Lei n.º 7/2004, de 7 de janeiro[14], que, no uso da autorização legislativa concedida pela Lei n.º 7/2003, de 9 de Maio, transpôs para a ordem jurídica nacional a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (versão consolidada).

Ao CNCS compete também garantir que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça. Importa neste particular aspeto ter em atenção a legislação concernente à proteção de dados pessoais e comunicações eletrónicas, nomeadamente:

- A Lei de proteção do utente de serviços públicos essenciais, aprovada pela Lei n.º 23/96, de 26 de julho[15], (versão consolidada). (Vd. trabalhos preparatórios);
- A Lei da proteção de dados pessoais, aprovada pela Lei n.º 67/98, de 26 de outubro[16] (versão consolidada). (Vd. trabalhos preparatórios);
- A Lei das comunicações eletrónicas, aprovada pela Lei n.º 5/2004, de 10 de fevereiro[17] (versão consolidada). (Vd. trabalhos preparatórios);
- A Lei relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, aprovada pela Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto. (Vd. trabalhos preparatórios da Lei n.º 41/2004 e os trabalhos preparatórios da Lei n.º 46/2012);
- A Lei relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, aprovada pela Lei n.º 32/2008, de 17 de julho. (Vd. trabalhos preparatórios);

[14] Alterado pelo Decreto-Lei n.º 62/2009, 10 de março, e pela Lei n.º 46/2012, de 29 de agosto.

[15] Alterada pelas Leis n.º 5/2004, de 10 de fevereiro, n.º 12/2008, de 26 de fevereiro, n.º 24/2008, de 2 de junho, n.º 6/2011, de 10 de março, n.º 44/2011, de 22 de junho, e n.º 10/2013, de 28 de janeiro.

[16] Retificada pela Declaração de Retificação n.º 22/98, de 28 de novembro e alterada pela Lei n.º 103/2015, de 24 de agosto.

[17] Retificada pela Declaração de Retificação n.º 32-A/2004, de 10 de abril, e alterada pelo Decreto-Lei n.º 258/2009, de 25 de setembro, pelas Leis n.º 46/2011, de 24 de junho, n.º 51/2011, de 13 de setembro, n.º 10/2013, de 28 de janeiro, n.º 42/2013, de 3 de julho, pelo Decreto-Lei n.º 35/2014, de 7 de março, pelas Leis n.º 82-B/2014, de 31 de dezembro, n.º 127/2015, de 3 de setembro, n.º 15/2016, de 17 de junho, e pelo Decreto-Lei n.º 92/2017, 31 de julho.

- A Lei relativa ao abuso sexual e exploração sexual de crianças e pornografia infantil, aprovada pela Lei n.º 103/2015, de 24 de agosto, e que procede à trigésima nona alteração ao Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, transpondo a Diretiva 2011/93/UE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, e cria o sistema de registo de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual de menor; primeira alteração à Lei n.º 113/2009, de 17 de setembro; primeira alteração à Lei n.º 67/98, de 26 de outubro, e segunda alteração à Lei n.º 37/2008, de 6 de agosto. (Vd. trabalhos preparatórios);
- Lei que regula e aprova o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficias do SIS e do SIED, aprovada pela Lei orgânica n.º 4/2017, de 25 de agosto. (Vd. trabalhos preparatórios).

A proposta de lei estabelece, ainda, um regime sancionatório próprio que remete para a aplicação subsidiária do regime geral das contraordenações, pelo que se torna pertinente referir o Decreto-Lei n.º 433/82, de 27 de outubro[18], que institui o ilícito de mera ordenação social, vulgarmente denominado como o Regime Geral das Contraordenações.

Relacionado com a matéria em apreço refira-se que, no âmbito do Plano Nacional para a Segurança dos Doentes 2015-2020, aprovado por Despacho n.º 1400-A/2015, de 2 de fevereiro, publicado no DR II Série n.º 28, de 10 de fevereiro de 2015, foi previsto como objetivo estratégico n.º 2 o "aumentar da segurança da comunicação". Ainda no âmbito da saúde, o Despacho n.º 1348/2017, de 27 de janeiro, publicado no DR II Série n.º 28, de 8 de fevereiro de 2017, determinou que entidades se encontram obrigadas a notificar incidentes de segurança, tendo designado o Responsável pela Notificação Obrigatória de incidentes de cibersegurança, e o Despacho n.º 8877/2017, de 29 de setembro, publicado no DR II Série n.º 197, de 9 de outubro, estabeleceu o modelo de governação relativo à implementação da política de cibersegurança da saúde.

Também o Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril, refere que o ciberterrorismo e a cibercriminalidade, podem ter "*por alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada*" como umas das ameaças e riscos à segurança nacional.

[18] Versão consolidada retirada do portal do DRE, elaborada a partir da republicação do diploma ocorrida com a aprovação do Decreto-Lei n.º 244/95, de 14 de setembro.

Quanto aos antecedentes parlamentares, é de referir a Resolução da Assembleia da República n.º 134/2017, de 28 de junho, a qual teve como origem os Projetos de Resolução n.º 778/XIII – CDS/PP e 852/XIII – PSD, e que Recomenda ao Governo que elabore as estratégias e os planos de ação decorrentes da Estratégia Nacional de Combate ao Terrorismo e aprove um plano de segurança para cada um dos aeroportos internacionais portugueses para a partilha de informação entre as respetivas administrações e as forças e serviços de segurança.

- **Enquadramento doutrinário/bibliográfico**

BARBOSA, Maria Luís – As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. **Revista de direito e segurança**. Lisboa. ISSN 2182-8687. A. 4, n.º 8 (jul./dez. 2016), p. 61-187. Cota: RP-301

Resumo: Atualmente, com a existência das redes de comunicação e do ciberespaço, a questão da segurança assume outras dimensões e termos que vão para lá do espaço físico e imediato. “Bens e serviços encontram-se agora disponíveis na rede e dependem desta para funcionar. A internet serve agora vários propósitos, possibilitando a troca instantânea de informação, a regulação de mercados, pagamentos e prestação de serviços, passando pelo fornecimento de bens essenciais, até à própria governação dos Estados. A vulnerabilidade de tais sistemas face a ataques cibernéticos e as repercussões que teriam na sociedade reforçam a importância da defesa e segurança do ciberespaço e das redes de comunicação. Sendo uma das grandes preocupações dos Estados, a cibersegurança passará pela projeção de estratégias que protejam não só os utilizadores, mas também o espaço virtual e físico do ciberespaço, assim como todas as infraestruturas e serviços que dele dependam”.

BENDIEK, Annegret; BOSSONG, Raphael; SCHULZE, Matthias – **The EU’s revised cybersecurity strategy** [Em linha] **: half-hearted progress on far-reaching challenges**. [S.l.] : German Institute for International and Security Affairs, 2017. [Consult. 04 abr. 2018]. Disponível em: WWW: <URL: http://catalogobib.parlamento.pt:81/images/winlibimg.aspx?skey=&doc=124436&img=8411&save=true

Resumo: Em setembro de 2017, a União Europeia atualizou a sua Estratégia de Segurança Cibernética de 2013. A nova versão destina-se a melhorar a proteção da infraestrutura crítica da Europa e a impulsionar a autoafirmação digital da UE, em relação a outras regiões do mundo. Contudo, esta nova estratégia deixa em aberto uma série de questões relativamente ao seu objetivo de um ciberespaço aberto e seguro, defendido de forma confiável, tanto interna como externamente.

Os autores afirmam que a União Europeia não definiu adequadamente, quer a resiliência, quer a dissuasão, nem deixou claro como pretende superar a fragmentação institucional e a falta de autoridade legal em questões de cibersegurança. Além disso, tópicos controversos, como a harmonização do direito penal ou o uso de criptografia, foram totalmente omitidos. Os autores apelam para que os Estados-membros abandonem os seus esforços independentes e acelerem a regulamentação legal da cibersegurança a nível da UE.

MARTINS, Marco – Ciberespaço : uma nova realidade para a segurança internacional. **Nação e defesa**. Lisboa. ISSN 0870-757X. N.º 133 (2012), p. 32-49. Cota: RP-72

Resumo: Segundo o autor, nos últimos anos tem-se vindo a assistir a novas formas de ameaças que cada vez mais se posicionam na rede cibernética, a nível internacional, provocando a deslocação do campo de batalha para o ciberespaço, representando a internet uma realidade incontornável das relações internacionais no quadro político e da segurança internacional. De facto, atualmente "não é possível afirmar a existência de um sistema de informação totalmente seguro e invulnerável". As novas tecnologias, ao mesmo tempo que revolucionaram o mundo, introduziram um fator negativo no que diz respeito à segurança, designadamente em questões de privacidade e garantia dos sistemas de informação do Estado.

PORTUGAL. Instituto da Defesa Nacional; ESPANHA. Centro Superior de Estudios de la Defensa Nacional – **Estratégia da informação e segurança no ciberespaço** [Em linha]. Lisboa: Instituto da Defesa Nacional, 2013. [Consult. 03 abr. 2018]. Disponível em: WWW: <URL: http://catalogobib.parlamento.pt:81/images/winlibimg.aspx?skey=&doc=124444&img=8420&save=true> ISBN 978-972-27-2272-8

Resumo: O presente estudo resultou da cooperação entre o Instituto da Defesa Nacional (IDN) de Portugal e da Escuela de Altos Estudios de la Defensa (EALEDE) do Centro Superior de Estudios de la Defensa Nacional (CESEDEN) de Espanha, relativamente à abordagem da cibersegurança.

São focados os seguintes tópicos: ciberespaço; conceito e âmbito de aplicação em segurança e defesa; estratégia de segurança da informação no ciberespaço; análise e gestão de riscos; infraestruturas críticas; ameaças; vulnerabilidades e boas práticas para a análise e gestão dos riscos; segurança da informação no ciberespaço e capacidade de resposta a incidentes informáticos; ciberdefesa e ciberexército. Procurou-se identificar pontos de convergência e refletir sobre a possibilidade de desenvolvimento futuro de iniciativas conjuntas, sobretudo de natureza bilateral, mas também multilateral, no quadro das organizações internacionais, em particular da NATO e da União Europeia.

UNIÃO EUROPEIA. Comissão Europeia – **Resilience, deterrance and defense** [Em linha] : **building strong cybersecurity for the EU**. Brussels : European Commission, 2017. [Consult. 03 abr. 2018]. Disponível em: WWW: <URL: http://catalogobib.parlamento.pt:81/images/winlibimg.aspx?skey=&doc=124438&img=8413&save=true

Resumo: A Diretiva sobre a Segurança de Redes e Sistemas de Informação (Diretiva (UE) 2016/1148) pretende criar uma cultura de segurança em sectores críticos para a economia e a sociedade, que dependam fortemente das tecnologias de informação e comunicação na União Europeia. Foi concebida com os seguintes objetivos: criar resiliência, melhorando as capacidades nacionais de segurança cibernética; fomentar uma melhor cooperação entre os Estados-membros; e exigir que empresas de setores económicos importantes adotem práticas eficazes de gestão de risco e notifiquem os incidentes graves às autoridades nacionais. A presente comunicação apresenta medidas específicas que reforçarão ainda mais as estruturas e capacidades da cibersegurança na União Europeia. A plena implementação da Diretiva por todos os Estados-membros, até maio de 2018, é essencial para a resiliência cibernética da UE.

UNIÃO EUROPEIA. Parlamento Europeu - Cybersecurity in the EU Common Security and Defense Policy (CSDP) [Em linha] : challenges and risks for the EU. Brussels : European Parliament, 2017. [Consult. 03 abr. 2018]. Disponível em: WWW: <URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf > ISBN 978-92-846-1058-7

Resumo: Este relatório é o resultado de um estudo realizado pela Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) para o Parlamento Europeu com o objetivo de identificar riscos, desafios e oportunidades para a defesa cibernética em contexto da Política Comum de Segurança e Defesa da UE (PCSD). O estudo gira em torno de três áreas temáticas, a saber: desafios políticos em matéria de ciberdefesa para os Estados-membros da UE, as instituições da UE, as partes interessadas a nível internacional e os decisores políticos. O segundo tema de pesquisa centra-se na capacitação, que inclui uma análise do estado da situação no cenário global entre nações, organizações internacionais e setor privado. O terceiro tema centra-se na PCSD e analisa os fatores-chave para o êxito da proteção das missões lideradas pela UE, civis e militares, contra as ameaças da cibercriminalidade.

WISER – Wide-Impact Cyber Security Risk Framework – **Essential guide to the Network and Information Security (NIS) Directive** [Em linha]. [S.l.] : WISER, 2016.

http://catalogobib.parlamento.pt:81/images/winlibimg.aspx?skey=&doc=124441&img=8416&save=true>

Resumo: A Diretiva relativa à segurança das redes e dos sistemas de informação (Diretiva NIS) representa a primeira regulamentação da UE em matéria de cibersegurança. Prevê-se que a referida Diretiva entre em vigor em agosto de 2016. Os Estados-membros terão 21 meses para transpor esta Diretiva para os respetivos ordenamentos jurídicos internos e mais 6 meses para identificar os operadores de serviços essenciais. O objetivo da Diretiva é alcançar um elevado nível comum de segurança dos sistemas de informação em rede na UE: melhorando as capacidades de cibersegurança a nível nacional; aumentando a cooperação a nível da União e tornando obrigatória a gestão de riscos e a elaboração de relatórios de incidentes para todos os operadores de serviços essenciais e provedores de serviços digitais.

- **Enquadramento do tema no plano da União Europeia**

Em 2004, a União Europeia criou a Agência Europeia para a Segurança das Redes e da Informação através do Regulamento (CE) n.º 460/2004, que tinha como objetivo primordial *garantir na Comunidade um nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público da União Europeia, contribuindo assim para o normal funcionamento do mercado interno.*

A Agência procurava sobretudo reforçar a capacidade da Comunidade, dos Estados-membros e da comunidade empresarial em matéria de prevenção, tratamento e resposta à segurança das redes e informação.

Segundo o Regulamento (UE) n.º 526/2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004, a ENISA tem um mandato, prorrogável, de 7 anos que termina em 2020, continuando o seu apoio às instituições europeias, Estados-membros e comunidade empresarial na análise, resposta e prevenção de problemas de segurança das redes e informação, através do conhecimento especializado, elaboração e execução de políticas da União, apoio ao reforço das suas capacidades, promoção da segurança na comunidade e capacitação.

Com o lançamento da primeira Estratégia da União Europeia para a Cibersegurança, foram definidos os princípios da cibersegurança e as prioridades estratégicas e ações neste campo: alcançar a resiliência do ciberespaço, reduzir a cibercriminalidade, desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da Política Comum de Segurança e Defesa, desenvolver recursos industriais e tecnológicos para a cibersegurança e estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia, promovendo os seus valores.

No mesmo sentido, a Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (SRI), e que agora se transpõe, estabelece a obrigação dos Estados-membros adotarem uma estratégia nacional de segurança de redes e sistemas de informação e cria um grupo de cooperação para facilitar a sua vertente estratégica e intercâmbio de informações, bem como uma rede de equipas de resposta a incidentes de segurança informática, requisitos de segurança e de notificação e ainda designação de autoridades nacionais competentes neste âmbito.

A Diretiva obriga os Estados-membros a identificarem, até 9 de novembro de 2018 os operadores de serviços essenciais de cada sector, estabelecidos no seu território, adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação, traçando objetivos estratégicos e medidas políticas e regulamentares adequadas para alcançar e manter um elevado nível de segurança, designarem autoridades nacionais competentes nesta matéria que controlarão a aplicação da Diretiva em causa a nível nacional, um ponto de contacto único e equipas de resposta a incidentes de segurança informática.

De referir ainda que o prazo de transposição da presente Diretiva termina no dia 9 de maio de 2018, conforme definido no seu artigo 25.º.

No que se refere ao Regulamento de Execução n.º 2018/151, este estabelece as normas de execução da Diretiva em apreço no que respeita à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial.

O Regulamento de Execução define assim os elementos de segurança, bem como os parâmetros que determinam se o impacto de um incidente é substancial, considerando um incidente de impacto substancial nos casos elencados no seu artigo 4.º.

A aplicabilidade deste regulamento inicia-se em 10 de maio de 2018.

Além da Diretiva em causa, em 2016, a Comunicação da Comissão sobre o reforço do sistema de ciberresiliência da Europa e a promoção de uma indústria de cibersegurança competitiva e inovadora referia-se ao aproveitamento pleno dos mecanismos de cooperação em matéria de SRI.

No que se refere ao tema em análise, a Assembleia da República escrutinou a Comunicação relativa à Proteção das infra-estruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial» (COM(2011)163), tendo sido objeto de relatório da Comissão para a Ética, Cidadania e Comunicação e posterior parecer da Comissão de Assuntos Europeus, bem como a Comunicação Conjunta relativa à Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido (COM(2013)1), objeto de relatório da Comissão para a Ética, Cidadania e Comunicação, Comissão de Defesa Nacional e Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, e parecer posterior da Comissão de Assuntos Europeus.

Foi ainda escrutinada a iniciativa que deu origem à Diretiva que se transpõe - Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União – COM(2013)48, tendo sido objeto de relatório por parte da Comissão para a Ética, a Cidadania e a Comunicação e da Comissão de Economia e Obras Públicas, bem como de parecer da Comissão de Assuntos Europeus.

- **Enquadramento internacional**

Países europeus

A legislação comparada é apresentada para os seguintes países da UE: Espanha, França e Reino Unido**.**

ESPANHA

O *Codigo de Derecho de la Ciberseguridad* espanhol contém o normativo principal referente à proteção do ciberespaço e à cibersegurança.

Além dos artigos da Constituição referentes à matéria das liberdades e da proteção dos direitos, por um lado, e aos princípios orientadores da política social e económica, por outro, o Código elenca um vasto conjunto de legislação pertinente, distribuída por diversos capítulos referentes à segurança nacional, às infraestruturas críticas, à equipa de resposta a incidentes de segurança, às telecomunicações, ao cibercrime, proteção de dados e relações com a administração.

De salientar que a Estratégia de Cibersegurança Nacional espanhola foi aprovada em dezembro de 2013 pelo Conselho de Segurança Nacional, e fixa como um dos objetivos principais «garantir um uso seguro das redes e dos sistemas de informação através do fortalecimento das (…) capacidades de prevenção, defesa, análise, investigação, recuperação e resposta os ciberataques», e reconhece o ciberespaço como um «novo âmbito de relação que proporcionou o desenvolvimento das novas tecnologias da informação e das comunicações, diluiu fronteiras, permitindo uma globalização sem precedentes, que proporciona novas oportunidades, mas acarreta sérios riscos e ameaças». A Estratégia fixa seis objetivos específicos, e entende a segurança nacional como uma ação do Estado dirigida a proteger os interesses nacionais, vitais e estratégicos relativos aos sistemas e infraestruturas de informação e telecomunicações comuns a todas as administrações públicas, infraestruturas críticas, capacidades militares e de defesa e todos os sistemas de interesse para a segurança nacional; para a liberdade e a segurança dos cidadãos; para a indústria; e para o património tecnológico.

O Plano Nacional de Cibersegurança constitui o primeiro nível de planificação da Estratégia e, seguindo as diretrizes gerais da mesma, identifica de forma mais exaustiva os riscos e as ameaças, os quais são depois vertidos no Relatório Anual de Segurança Nacional que é posteriormente apresentado ao Congresso.

Refira-se que a Diretiva (UE) n.º 2016/1148 se encontra em fase de transposição para o ordenamento jurídico espanhol, tendo o Ministério de Energia, Turismo e Agenda Digital procedido, no início do presente ano, à submissão a audiência pública do anteprojeto de lei (*Anteproyectro de ley sobre la seguridad de las redes y sistemas de información*) com vista à sua transposição, podendo a respetiva análise do impacto normativo ser consultada aqui.

O Instituto Nacional de Segurança Cibernética de Espanha (INCIBE), anteriormente Instituto Nacional de Tecnologias de Comunicação, foi criado no âmbito da Secretaria de Estado da Sociedade da Informação e da Agenda Digital (SESIAD) constitui uma entidade de referência para o desenvolvimento da cibersegurança e confiança digital dos cidadãos, rede académica e de investigação, profissionais, empresas e, principalmente, para setores estratégicos. Com uma atividade baseada na investigação, na prestação de serviços e na coordenação com os agentes com competências na área, o INCIBE contribui para a construção da cibersegurança ao nível nacional e internacional.

FRANÇA

A Diretiva (UE) n.º 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 da informação em toda a União foi já transposta para o ordenamento jurídico francês através da *Loi* n.º 2018-133, de 26 de fevereiro, *portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*.

Já, anteriormente, se encontrava prevista a proteção de determinados sistemas de informação crítica pela Lei de Programação Militar para 2014-2019 (*Loi* n ° 2013-1168, de 18 de dezembro).
A transposição desta Diretiva constituiu numa oportunidade de impor a outros operadores (*e.g*. a sociedade e a economia) obrigações básicas de segurança digital. Além disso, a *Loi* n.º 2018-133 aplica-se expressamente a operadores que não estejam classificados de importância vital, ou sendo operadores de importância vital, não tenham a parte do seu sistema de informação classificado como importância vital (artigo 5 al. 2 da *Loi* que remete, respetivamente, para os artigos L.1332-1 e L.1332-2 e artigo L.1332-6-1 do *Code de la défense*).

O Capítulo I da *Loi* n.º 2018-133 trata de «redes e sistemas de informação». A definição de redes de comunicações eletrónicas remete para a que consta no *Code des Postes et des Communications Électroniques* (CPCE) (artigo L.32). A definição de processamento automatizado de dados digitais abrange todos os elementos de *hardware* e *software* que lidam com dados digitais, sejam ou não dados pessoais, sem, no entanto fazer referência à noção de sistema automatizado de processamento de dados previsto nos artigos 323. -1 a 323-3 do Código Penal.
Os dados digitais em causa consistem em todos os dados armazenados, processados, recuperados ou transmitidos numa rede de comunicações eletrónicas ou num dispositivo automatizado de processamento digital de dados. A noção de segurança prevista no artigo 1 da *Loi n.º* 2018-133 consiste na «capacidade de resistir, num dado nível de confiança, a ações que comprometam a disponibilidade, a autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou processados».

O artigo 2º da *Loi n.º* 2018-133 especifica, em primeiro lugar, os operadores que estão isentos das obrigações de segurança das redes e sistemas de informação, sendo eles os operadores na aceção do artigo L.32-15° do CPCE e os prestadores cobertos pelo Regulamento da UE n.º 2014/910, de 23 de julho 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

Os operadores de serviços essenciais não abrangidos pelos artigos 1.º a 4.º do Capítulo I da lei estão sujeitos ao previsto no Capítulo II.
A definição do requisito de segurança para redes de comunicações eletrónicas e dispositivos de processamento automatizado de dados digitais aguarda a legislação complementar a ser aprovada o mais tardar em 10 de maio de 2018, nos termos do artigo 4.º da *Loi n.º* 2018-133.

Quanto aos operadores de serviços essenciais, que representam a grande novidade desta Diretiva transposta, constam do Capítulo II («Disposições relativas à segurança de redes e sistemas de informação de operadores de serviços essenciais»). São eles operadores, públicos ou privados, que prestam serviços essenciais ao funcionamento da sociedade ou da economia e cuja continuidade pode ser seriamente afetada por incidentes que afetam as redes e os sistemas de informação necessários à prestação de tais serviços. São designados pelo Primeiro-Ministro, ou, por delegação, pela *Agence Nationale de le Sécurité des Systèmes d'Information* (ANSSI), o mais tardar até 9 de novembro de 2018, nos termos do artigo 25.º («Disposições transitórias») da Lei.
A obrigação de segurança para operadores de serviços essenciais será definida pela ANSSI, nos termos do artigo 6º da Lei, o qual estabelece apenas alguns princípios.

A implementação de medidas de segurança obrigatórias será efetuada às custas dessas empresas classificadas como «Operadores de Serviços Essenciais» ou como «Operadores de Importância Vital».

As regras de segurança necessárias para a proteção de redes e sistemas de informação garantem um nível de segurança adaptado ao risco existente, tendo em conta o «estado da arte». O diploma de desenvolvimento deve especificar as medidas adequadas para evitar incidentes que comprometam a segurança de redes e sistemas de informação utilizados para a prestação de serviços essenciais ou para limitar o impacto, a fim de assegurar a continuidade da prestação destes serviços essenciais.

Os incidentes que afetam as redes e sistemas de informação necessários para a prestação de serviços essenciais são notificados à ANSSI (artigo 7.º, I.º da Lei), que não terá que relatar todos os incidentes, mas apenas aqueles que terão um impacto significativo na continuidade desses serviços.

As sanções por violação das obrigações de segurança das redes e dos sistemas de informação aplicam-se aos responsáveis dos operadores de serviços essenciais e não à pessoa coletiva. As multas variam de 75.000,00 a 125.000,00 Euros (artigo 9.º).

O Capítulo III debruça-se sobre a «Segurança de Redes e Sistemas de Informação de Prestadores de Serviços Digitais». Nos termos do artigo 10.º, um serviço digital consiste num serviço normalmente prestado mediante remuneração, remotamente, eletronicamente e a pedido individual de um destinatário de serviços. O operador de um serviço digital é qualquer pessoa jurídica que forneça um desses serviços. Esta definição visa expressamente e limitativamente três (3) tipos de prestadores: (i) «mercados *on-line*», que permitem que qualquer pessoa, operador económico ou não, conclua contratos de vendas ou de serviços *on-line* com profissionais no sítio do local, ou no sítio de um profissional que utiliza os serviços de informática fornecidos pelo mercado *on-line*. (ii) «motores de busca *on-line*» considerado como um serviço digital que permite aos utilizadores pesquisar, em princípio, todos os sítios ou sítios de um determinado idioma, com base numa consulta sobre qualquer assunto na forma de uma palavra-chave, frase ou outra entrada, e que a partir do qual é possível encontrar informações relacionadas ao conteúdo solicitado. (iii) «serviços de computação em nuvem», como sendo um serviço digital que permite o acesso a um conjunto flexível e variável de recursos de computação que pode ser compartilhado.

O prestador tem que oferecer um serviço na União Europeia (UE). Se tiver a sua sede registada ou o principal local de negócios situado no território francês, é considerado um prestador de serviços digitais, de acordo com a *Loi n.º* 2018-133. Se estiver localizada fora da UE ou não tiver nenhum representante noutro país da UE, será obrigada a indicar um.

A *Loi n.º* 2018-133 não se aplica a empresas com menos de 50 empregados e cujo volume de negócios não exceda 10 milhões de euros (artigo 11.º, III), sendo que os requisitos são cumulativos.

O requisito de segurança para redes e sistemas de informação para prestadores de serviços digitais deve garantir, tendo em conta o «estado da arte», um nível de segurança necessário para a prestação dos seus serviços na UE, adaptado aos riscos existentes (artigo 12.º).

À semelhança dos operadores de serviços essenciais, também os prestadores de serviços digitais são obrigados a notificar a ANSSI de qualquer incidente de segurança tendo um impacto significativo na prestação do serviço, estando sujeitos às multas previstas no artigo 15.º em caso de incumprimento dos requisitos de segurança.

As multas variam de 50.000,00 Euros a 100.000,00 Euros (um pouco menos do que para os operadores de serviços essenciais).

Refira-se, também, conforme estabelecido na *Loi n.º* 2013-1168, de 18 de dezembro (Lei da Programação Militar), que o Primeiro-Ministro define a política e coordena a ação do governo em questões de segurança e defesa dos sistemas de informação. Para tal existe a já citada *Agence nationale de sécurité des systèmes d'information* (ANSSI), que reporta ao Secretário-Geral de Defesa e Segurança Nacional, e que consiste na autoridade nacional para estas matérias. A ANSSI produziu a Estratégia Nacional para a Segurança Digital e ainda a Estratégia francesa para a Defesa e segurança dos sistemas de informação.

A Estratégia Nacional para a Segurança Digital responde aos novos desafios decorrentes da evolução do digital e das ameaças, relativas a cinco objetivos: garantir a soberania nacional; fornecer uma resposta forte contra os ataques cibernéticos; informar o público em geral; tornar segurança digital uma vantagem competitiva para empresas francesas; e fortalecer internacionalmente a França.

REINO UNIDO

Em junho de 2016 teve lugar o referendo na sequência do qual o Reino Unido escolheu sair da UE. No entanto, até que as negociações de saída fiquem concluídas, o Reino Unido é membro de pleno direito da UE, pelo que todos os direitos e obrigações mantêm-se em vigor. Durante este período, o governo britânico continua a negociar, a implementar e a aplicar a legislação europeia.

Assim, em agosto de 2017 o governo submeteu[19] a consulta pública a sua proposta de melhoraria da segurança dos serviços essenciais do país, através da transposição da Diretiva (UE) n.º 2016/1148. Esta consulta abrangeu seis tópicos principais: como identificar os serviços essenciais; a constituição de uma estrutura nacional para gerir a sua implementação; os requisitos de segurança para operadores de serviços essenciais; os requisitos do relatório de incidentes para operadores de serviços essenciais; os requisitos sobre os fornecedores de serviços digitais; o regime de sanções proposto.

Da consulta pública[20] resultaram como principais conclusões, e que constituem as áreas de preocupação da atuação do governo nesta matéria, o seguinte:

[19] Através do *Department for Digital, Culture, Media and Sport* (DCMS).

[20] O relatório da consulta pública encontra-se disponível aqui.

1) A definição dos critérios para a identificação dos operadores de serviços essenciais, tendo ficado assente que os fornecedores de serviços digitais são aqueles que se encontram já previstos na Diretiva.

2) O papel da autoridade competente e a forma como tem lugar a delegação de poderes. Ficou definido que, ao abrigo do novo regime decorrente da transposição da Diretiva, diferentes autoridades competentes terão a responsabilidade de monitorizar a conformidade e a execução dos sistemas de segurança, dependendo das organizações do sector em causa. Assim, os ministros da energia, da saúde e dos transportes, por exemplo, agirão como autoridades competentes, bem como os reguladores do setor e a entidade de proteção de dados (*Information Commissioner Officer*).

De salientar que o governo decidiu isentar deste regime as empresas que operam na infraestrutura dos mercados financeiros e bancários, sob o argumento de que já existem «atos jurídicos da UE» que estabelecem requisitos específicos para o setor quanto à segurança da rede e dos sistemas de informação das empresas ou à notificação de incidentes de cibersegurança. As empresas do setor devem continuar a cumprir os requisitos-padrão estabelecidos pelo *Bank of England* e/ou pela *Financial Conduct Authority*.

Resulta ainda da consulta efetuada a intenção do governo de atualizar a legislação nacional, codificando os requisitos de reporte de incidentes de modo a harmonizar a regulamentação de segurança cibernética das infraestruturas do mercado financeiro a regulamentações equivalentes que serão introduzidas nos restantes setores na sequência da transposição da Diretiva (UE) n.º 2016/1148.

3) O *National Cyber Security Centre* (NCSC) que aprovou um guia para os operadores de serviços essenciais sobre o tipo de medidas de segurança a implementar, ficou com as suas funções circunscritas à segurança cibernética.

4) O governo pretende também simplificar o regime de resposta a incidentes, separar os procedimentos de resposta a incidentes dos procedimentos de notificação de incidentes, e o regime de sanções de modo a reduzir o risco de coimas superiores a 17 milhões de libras. O sistema sancionatório só servirá como dissuasor e não serão emitidas multas quando os operadores de serviços essenciais tiverem avaliado adequadamente os riscos, adotado as

medidas de segurança apropriadas e articulado com os reguladores, mas ainda assim tenham sofrido um ataque.

O governo reconhece a possibilidade dos operadores de serviços essenciais que violem as regras decorrentes da aplicação da Diretiva possam, também, violar simultaneamente outra legislação e admitiu que pudessem receber mais do que uma multa oriunda de diferentes reguladores em relação à violação da mesma regra de segurança. O princípio é o de que os operadores de serviços essenciais e os fornecedores de serviços digitais não devam ser condenados duplamente pela mesma infração, mas admite que possa haver uma razão para serem sancionados, pelo mesmo evento, sob regimes diferentes porque as sanções podem estar relacionadas com diferentes aspetos da infração e a impactos diferentes.
Admitindo que não é possível evitar essa dupla penalização sem prejudicar a aplicação da Diretiva, a opção política foi a de encorajar as autoridades competentes a trabalhar com os reguladores no caso de haver diferentes regimes aplicáveis a fim de determinar a abordagem a ser adotada. Tal não limitará a capacidade da autoridade competente em aplicar a sanção adequada às circunstâncias, mas incentivará a consideração de outros regimes.

Destacam-se conexos com a matéria em apreço, o *Data Protection Act*, e os *Privacy and Electronic Communications Regulations*. Existem ainda bastantes guias práticos, situados num plano regulamentar, com orientações específicas sobre a matéria, tanto para organizações como para cidadãos os quais podem ser encontrados no portal do *Information Commisioner Office*.

Pertinente para consulta, o *National Cyber Security Strategy 2016-2020* tem também uma versão oficial em língua portuguesa.

Organizações internacionais

CONSELHO DA EUROPA

Concluída e aprovada em novembro de 2001, a Convenção sobre o Cibercrime foi apresentada para assinatura e ratificação aos 47 Estados-membros, bem como a outros Estados presentes com o estatuto de observador, entre os quais Estados Unidos da América, Japão, África do Sul e Canadá. Foi ainda acrescentado um protocolo adicional em janeiro de 2003 com o intuito de abordar as questões de natureza racista e xenófobas no ciberespaço: *Additional Protocol to the Convention on*

Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Até à data só não foi assinada pela Federação Russa, não tendo ainda sido ratificada pela Irlanda, Suécia e África do Sul. Esta Convenção entrou em vigor a dia 1 de julho de 2004 após ser ratificada por 5 países, dos quais 3 são Estados-membros do Conselho de Europa.

Em Portugal, a Convenção foi aprovada pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro, com a manifestação de reserva ao n.º 5 do artigo 24.º, sobre os «Princípios gerais relativos ao auxílio judiciário mútuo».

IV. Iniciativas legislativas e petições pendentes sobre a mesma matéria

- **Iniciativas legislativas**

Efetuada consulta à base de dados da Atividade Parlamentar (AP), verificou-se que, neste momento, não se encontra pendente qualquer iniciativa ou petição sobre a mesma matéria.

V. Consultas e contributos

A Comissão solicitou, em 04 de abril de 2018, parecer escrito às seguintes entidades: Comissão Nacional de Proteção de Dados, Conselho Superior do Ministério Público, Gabinete Nacional de Segurança e Comissão de Acesso aos Documentos Administrativos.

O Presidente da Assembleia da República promoveu, em 02 de abril de 2018, a audição dos órgãos de governo próprios das regiões autónomas, nos termos do artigo 142.º do Regimento da Assembleia da República, e para os efeitos do n.º 2 do artigo 229.º da Constituição.

Os pareceres serão disponibilizados no *site* da Assembleia da República, mais especificamente na página eletrónica da presente iniciativa.

VI. Apreciação das consequências da aprovação e dos previsíveis encargos com a sua aplicação

Em face da informação disponível, não é possível determinar eventuais encargos resultantes da aprovação da presente iniciativa. Contudo, da respetiva aplicação parecem decorrer os encargos inerentes ao cumprimento de medidas técnicas e organizativas adequadas e proporcionais, pela Administração Pública e pelos operadores de infraestruturas críticas, bem como a eventual reorganização do Centro Nacional de Cibersegurança. Por outro lado, o incumprimento das normas implica a aplicação de coimas que revertem 60% para o Estado e 40% para o Centro.