ASSEMBLEIA DA REPÚBLICA

Lei n.º 46/2018

de 13 de agosto

Estabelece o regime jurídico da segurança do ciberespaço, transpondo 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.

A Assembleia da República decreta, nos termos da alínea *c*) do artigo 161.º da Constituição, o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

A presente lei estabelece o regime jurídico da segurança do ciberespaço, transpondo 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.

Artigo 2.º

Âmbito

1 — A presente lei aplica-se:

a) À Administração Pública;
b) Aos operadores de infraestruturas críticas;
c) Aos operadores de serviços essenciais;
d) Aos prestadores de serviços digitais;
e) A quaisquer outras entidades que utilizem redes e sistemas de informação.

2 — Para efeitos do disposto na presente lei, integram a Administração Pública:

a) O Estado;
b) As regiões autónomas;
c) As autarquias locais;
d) As entidades administrativas independentes;
e) Os institutos públicos;
f) As empresas públicas;
g) As associações públicas.

3 — A presente lei aplica-se aos prestadores de serviços digitais que tenham o seu estabelecimento principal em território nacional ou, não o tendo, designem um representante estabelecido em território nacional, desde que aí prestem serviços digitais.

4 — Para efeitos do número anterior, considera-se que um prestador de serviços digitais tem o seu estabelecimento principal em território nacional quando aí tiver a sua sede.

5 — Caso uma entidade se enquadre simultaneamente em mais do que uma das alíneas *a*) a *c*) do n.º 1, aplica-se o regime que resultar mais exigente para a segurança das redes e dos sistemas de informação.

6 — A presente lei não se aplica:

a) 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;
b) Às redes e sistemas de informação que processem informação classificada.

7 — O disposto na presente lei não prejudica o cumprimento da legislação aplicável em matéria:

a) De proteção de dados pessoais, designadamente o disposto no Regulamento (UE) n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), e na Lei n.º 26/2016, de 22 de agosto;
b) De identificação e designação de infraestruturas críticas nacionais e europeias, designadamente do Decreto-Lei n.º 62/2011, de 9 de maio;
c) De luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, designadamente da Lei n.º 103/2015, de 24 de agosto;
d) De proteção do utente de serviços públicos essenciais, designadamente da Lei n.º 23/96, de 26 de julho;
e) De segurança e de emergência no setor das comunicações eletrónicas, designadamente da Lei n.º 5/2004, de 10 de fevereiro.

8 — A presente lei não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais.

Artigo 3.º

Definições

Para efeitos da presente lei, entende-se por:

a) «Equipa de resposta a incidentes de segurança informática», a equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação;
b) «Especificação técnica», um documento que define os requisitos técnicos que um produto, processo, serviço ou sistema devem cumprir;
c) «Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;
d) «Infraestrutura crítica», a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções;
e) «Norma», uma especificação técnica, aprovada por um organismo de normalização reconhecido, para aplicação repetida ou continuada, cuja observância não é obrigatória;
f) «Operador de infraestrutura crítica», uma entidade pública ou privada que opera uma infraestrutura crítica;
g) «Operador de serviços essenciais», uma entidade pública ou privada que presta um serviço essencial;
h) «Ponto de troca de tráfego», uma estrutura de rede que permite a interligação de mais de dois sistemas autó-

nomos independentes a fim de facilitar a troca de tráfego na *Internet;*

i) «Prestador de serviços digitais», uma pessoa coletiva que presta um serviço digital;

j) «Prestador de serviços do sistema de nomes de domínio», uma entidade que presta serviços do sistema de nomes de domínio (DNS) na *Internet*;

k) «Rede e sistema de informação», 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;

l) «Registo de nomes de domínio de topo», uma entidade que administra e opera o registo de nomes de domínio da *Internet* de um domínio de topo específico;

m) «Representante do prestador de serviços digitais», uma pessoa singular ou coletiva, estabelecida na União Europeia, expressamente designada para atuar por conta de um prestador de serviços digitais aí não estabelecido;

n) «Risco», uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação;

o) «Segurança das redes e dos sistemas de informação», a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles;

p) «Serviço de computação em nuvem», um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis;

q) «Serviço de mercado em linha», um serviço digital que permite aos consumidores ou aos comerciantes celebrarem contratos de venda ou de prestação de serviços por via eletrónica com comerciantes, quer no sítio na *Internet* do mercado em linha, quer no sítio na *Internet* de um comerciante que utilize os serviços de computação disponibilizados pelo mercado em linha;

r) «Serviço de motor de pesquisa em linha», um serviço digital que permite aos utilizadores consultarem todos os sítios na *Internet*, ou sítios na *Internet* numa determinada língua, com base numa pesquisa sobre qualquer assunto e que fornece ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado;

s) «Serviço digital», um serviço da sociedade da informação prestado à distância, por via eletrónica;

t) «Serviço essencial», um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço;

u) «Sistema de nomes de domínio» (DNS), um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio;

v) «Tratamento de incidentes», todos os procedimentos de apoio à deteção, análise, contenção e resposta a um incidente.

Artigo 4.º

Estratégia Nacional de Segurança do Ciberespaço

1 — A Estratégia Nacional de Segurança do Ciberespaço define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional.

2 — A Estratégia Nacional de Segurança do Ciberespaço é aprovada por resolução do Conselho de Ministros, sob proposta do Primeiro-Ministro, ouvido o Conselho Superior de Segurança do Ciberespaço.

CAPÍTULO II

Estrutura de segurança do ciberespaço

Artigo 5.º

Conselho Superior de Segurança do Ciberespaço

1 — O Conselho Superior de Segurança do Ciberespaço é o órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço.

2 — O Conselho Superior de Segurança do Ciberespaço tem a seguinte composição:

a) O membro do Governo responsável pela área da cibersegurança, que preside;

b) A Autoridade Nacional de Segurança, que substitui o presidente nas suas ausências e impedimentos;

c) O Secretário-Geral do Sistema de Segurança Interna;

d) O Secretário-Geral do Sistema de Informações da República Portuguesa;

e) Dois Deputados designados pela Assembleia da República através do método de *Hondt*;

f) O Diretor do Serviço de Informações de Segurança;

g) O Diretor do Serviço de Informações Estratégicas de Defesa;

h) O Coordenador do Centro Nacional de Cibersegurança;

i) O Embaixador para a ciberdiplomacia;

j) Um representante da área da administração eleitoral;

k) O Presidente do Conselho Diretivo da Agência para a Modernização Administrativa, I. P.;

l) O Diretor-Geral da Autoridade Tributária e Aduaneira;

m) O Diretor do Centro de Gestão da Rede Informática do Governo;

n) O Presidente do Conselho Diretivo da Entidade de Serviços Partilhados da Administração Pública, I. P.;

o) O Diretor de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas;

p) Um representante da Rede Nacional de Segurança Interna;

q) O Presidente do Instituto de Gestão Financeira e Equipamentos da Justiça, I. P.;

r) O Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária;

s) Um representante do Ministério Público designado pelo Procurador-Geral da República;

t) O Presidente da Fundação para a Ciência e a Tecnologia, I. P.;

u) O Diretor-Geral de Educação;

v) O Presidente do Conselho de Administração da SPMS — Serviços Partilhados do Ministério da Saúde, E. P. E.;

w) O Presidente do Conselho de Administração Executivo da Infraestruturas de Portugal, S. A.;

x) O Presidente do Conselho Diretivo do IAPMEI — Agência para a Competitividade e Inovação, I. P.;

y) O Presidente do Conselho de Administração da Autoridade Nacional de Comunicações;

z) Um representante da Direção de Recursos Naturais, Segurança e Serviços Marítimos;

aa) Um representante da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática.

3 — A composição do Conselho Superior de Segurança do Ciberespaço inclui também um representante do governo da Região Autónoma dos Açores e um representante do governo da Região Autónoma da Madeira.

4 — O presidente, por sua iniciativa ou a pedido de qualquer dos membros do Conselho, pode convocar outros titulares de órgãos públicos ou convidar outras personalidades de reconhecido mérito para participar em reuniões do Conselho Superior de Segurança do Ciberespaço.

Artigo 6.º

Competências do Conselho Superior de Segurança do Ciberespaço

1 — Compete ao Conselho Superior de Segurança do Ciberespaço:

a) Assegurar a coordenação político-estratégica para a segurança do ciberespaço;

b) Verificar a implementação da Estratégia Nacional de Segurança do Ciberespaço;

c) Pronunciar-se sobre a Estratégia Nacional de Segurança do Ciberespaço previamente à sua submissão para aprovação;

d) Elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço;

e) Propor ao Primeiro-Ministro, ou ao membro do Governo em quem este delegar, a aprovação de decisões de carácter programático relacionadas com a definição e execução da Estratégia Nacional de Segurança do Ciberespaço;

f) Emitir parecer sobre matérias relativas à segurança do ciberespaço;

g) Responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem este delegar, no âmbito das suas competências.

2 — O relatório anual de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço é enviado à Assembleia da República até 31 de março do ano posterior àquele a que se reporta.

Artigo 7.º

Centro Nacional de Cibersegurança

1 — O Centro Nacional de Cibersegurança funciona no âmbito do Gabinete Nacional de Segurança e é a Autoridade Nacional de Cibersegurança.

2 — O Centro Nacional de Cibersegurança 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.

3 — O Centro Nacional de Cibersegurança é o ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais da Polícia Judiciária relativas a cooperação internacional em matéria penal.

4 — O Centro Nacional de Cibersegurança exerce as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias nos termos das suas competências.

5 — O Centro Nacional de Cibersegurança tem o poder de emitir instruções de cibersegurança e de definir o nível nacional de alerta de cibersegurança.

6 — Qualquer disposição legal de cibersegurança carece do parecer prévio do Centro Nacional de Cibersegurança.

7 — O Centro Nacional de Cibersegurança atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à autoridade competente, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

8 — O Centro Nacional de Cibersegurança atua em articulação com a Comissão Nacional de Proteção de Dados quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais.

9 — O Centro Nacional de Cibersegurança pode solicitar a quaisquer entidades públicas ou privadas toda a colaboração ou auxílio que julgue necessários para o exercício das suas atividades.

Artigo 8.º

Equipa de Resposta a Incidentes de Segurança Informática Nacional

1 — A Equipa de Resposta a Incidentes de Segurança Informática Nacional é o «CERT.PT».

2 — O «CERT.PT» funciona no Centro Nacional de Cibersegurança.

Artigo 9.º

Competências do «CERT.PT»

O «CERT.PT» possui as seguintes competências:

a) Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes;

b) Monitorizar os incidentes com implicações a nível nacional;

c) Ativar mecanismos de alerta rápido;

d) Intervir na reação, análise e mitigação de incidentes;

e) Proceder à análise dinâmica dos riscos;

f) Assegurar a cooperação com entidades públicas e privadas;

g) Promover a adoção e a utilização de práticas comuns ou normalizadas;
h) Participar nos *fora* nacionais de cooperação de equipas de resposta a incidentes de segurança informática;
i) Assegurar a representação nacional nos *fora* internacionais de cooperação de equipas de resposta a incidentes de segurança informática;
j) Participar em eventos de treino nacionais e internacionais.

Artigo 10.º

Operadores de serviços essenciais

Os operadores de serviços essenciais enquadram-se num dos tipos de entidades que atuam nos setores e subsetores constantes do anexo à presente lei, da qual faz parte integrante.

Artigo 11.º

Prestadores de serviços digitais

Os prestadores de serviços digitais prestam os seguintes serviços:

a) Serviço de mercado em linha;
b) Serviço de motor de pesquisa em linha;
c) Serviço de computação em nuvem.

CAPÍTULO III

Segurança das redes e dos sistemas de informação

Artigo 12.º

Definição de requisitos de segurança e normalização

1 — Os requisitos de segurança são definidos nos termos previstos em legislação própria, sem prejuízo do disposto no artigo 18.º
2 — Os requisitos de segurança não se aplicam:

a) Às empresas sujeitas aos requisitos previstos nos artigos 54.º-A a 54.º-G da lei das comunicações eletrónicas, aprovada pela Lei n.º 5/2004, de 10 de fevereiro, na sua redação atual;
b) Aos prestadores de serviços de confiança previstos no artigo 19.º do Regulamento (UE) n.º 910/2014, de 23 de julho, do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

3 — Os requisitos de segurança são definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

Artigo 13.º

Definição de requisitos de notificação de incidentes

1 — Os requisitos de notificação de incidentes são definidos nos termos previstos em legislação própria, sem prejuízo do disposto no artigo 19.º
2 — Os requisitos de notificação de incidentes não se aplicam:

a) Às empresas sujeitas aos requisitos previstos nos artigos 54.º-A a 54.º-G da lei das comunicações eletrónicas, aprovada pela Lei n.º 5/2004, de 10 de fevereiro, na sua redação atual;
b) Aos prestadores de serviços de confiança previstos no artigo 19.º do Regulamento (UE) n.º 910/2014, de 23 de julho, do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

Artigo 14.º

Requisitos de segurança para a Administração Pública e operadores de infraestruturas críticas

1 — A Administração Pública e os operadores de infraestruturas críticas devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.
2 — As medidas previstas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.
3 — A Administração Pública e os operadores de infraestruturas críticas tomam as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto.

Artigo 15.º

Notificação de incidentes para a Administração Pública e operadores de infraestruturas críticas

1 — A Administração Pública e os operadores de infraestruturas críticas notificam o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na segurança das redes e dos sistemas de informação, no prazo definido na legislação própria referida no artigo 13.º
2 — A notificação dos operadores de infraestruturas críticas inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço dos incidentes.
3 — A notificação não acarreta responsabilidades acrescidas para a parte notificante.
4 — A fim de determinar a relevância do impacto de um incidente são tidos em conta, designadamente, os seguintes parâmetros:

a) O número de utilizadores afetados;
b) A duração do incidente;
c) A distribuição geográfica, no que se refere à zona afetada pelo incidente.

5 — Sempre que as circunstâncias o permitam, o Centro Nacional de Cibersegurança presta ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente.
6 — O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos operadores de infraestruturas críticas.

Artigo 16.º

Requisitos de segurança para os operadores de serviços essenciais

1 — Os operadores de serviços essenciais devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.

2 — As medidas previstas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.

3 — Os operadores de serviços essenciais tomam as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados para a prestação dos seus serviços essenciais e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.

Artigo 17.º

Notificação de incidentes para os operadores de serviços essenciais

1 — Os operadores de serviços essenciais notificam o Centro Nacional de Cibersegurança dos incidentes com um impacto relevante na continuidade dos serviços essenciais por si prestados, no prazo definido na legislação própria referida no artigo 13.º

2 — A notificação inclui informação que permita ao Centro Nacional de Cibersegurança determinar o impacto transfronteiriço dos incidentes.

3 — A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4 — A fim de determinar a relevância do impacto de um incidente são tidos em conta, designadamente, os seguintes parâmetros:

a) O número de utilizadores afetados pela perturbação do serviço essencial;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente.

5 — Com base na informação prestada na notificação, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos dos outros Estados-Membros afetados, caso o incidente tenha um impacto importante na continuidade dos serviços essenciais nesses Estados-Membros.

6 — No caso referido no número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do operador de serviços essenciais, bem como a confidencialidade da informação prestada na sua notificação.

7 — Sempre que as circunstâncias o permitam, o Centro Nacional de Cibersegurança presta ao operador de serviços essenciais notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente.

8 — O Centro Nacional de Cibersegurança transmite as notificações referidas no n.º 1 aos pontos de contacto únicos dos outros Estados-Membros afetados.

9 — O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar informação relativa a incidentes específicos de acordo com o interesse público.

10 — Se um operador de serviços essenciais depender de um terceiro prestador de serviços digitais para a prestação de um serviço essencial, notifica todos os impactos importantes na continuidade dos seus serviços, decorrentes dos incidentes que afetem o prestador de serviços digitais.

Artigo 18.º

Requisitos de segurança para os prestadores de serviços digitais

1 — Os prestadores de serviços digitais identificam e tomam as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam no contexto da oferta dos serviços digitais.

2 — As medidas referidas no número anterior devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, e devem ter em conta os seguintes fatores:

a) A segurança dos sistemas e das instalações;

b) O tratamento dos incidentes;

c) A gestão da continuidade das atividades;

d) O acompanhamento, a auditoria e os testes realizados;

e) A conformidade com as normas internacionais.

3 — Os prestadores de serviços digitais tomam medidas para evitar os incidentes que afetem a segurança das suas redes e sistemas de informação e para reduzir ao mínimo o seu impacto nos serviços digitais, a fim de assegurar a continuidade desses serviços.

4 — O presente artigo não se aplica às microempresas nem às pequenas empresas, tal como definidas pelo Decreto-Lei n.º 372/2007, de 6 de novembro, na sua redação atual.

5 — Os elementos constantes dos n.os 1 a 3 são objeto de Regulamento de Execução da Comissão Europeia.

Artigo 19.º

Notificação de incidentes para os prestadores de serviços digitais

1 — Os prestadores de serviços digitais notificam o Centro Nacional de Cibersegurança dos incidentes com impacto substancial na prestação dos serviços digitais, no prazo definido na legislação própria referida no artigo 13.º

2 — A notificação referida no número anterior inclui informação que permita ao Centro Nacional de Cibersegurança determinar a importância dos impactos transfronteiriços.

3 — A notificação não acarreta responsabilidades acrescidas para a parte notificante.

4 — A fim de determinar se o impacto de um incidente é substancial, são tidos em conta os seguintes parâmetros:

a) O número de utilizadores afetados pelo incidente, nomeadamente de utilizadores que dependem do serviço para prestarem os seus próprios serviços;

b) A duração do incidente;

c) A distribuição geográfica, no que se refere à zona afetada pelo incidente;

d) O nível de gravidade da perturbação do funcionamento do serviço;

e) A extensão do impacto nas atividades económicas e societais.

5 — A obrigação de notificar um incidente só se aplica se o prestador de serviços digitais tiver acesso a informação necessária para avaliar o impacto de um incidente em função dos fatores a que se refere o n.º 2 do artigo anterior.

6 — Se os incidentes referidos no n.º 1 disserem respeito a dois ou mais Estados-Membros, o Centro Nacional de Cibersegurança informa os pontos de contacto únicos dos outros Estados-Membros afetados.

7 — No caso referido no número anterior, o Centro Nacional de Cibersegurança salvaguarda a segurança e os interesses do prestador de serviços digitais.

8 — O Centro Nacional de Cibersegurança, após consultar o notificante, pode divulgar incidentes específicos de acordo com o interesse público.

9 — O presente artigo não se aplica às microempresas nem às pequenas empresas, tal como definidas pelo Decreto-Lei n.º 372/2007, de 6 de novembro, na sua redação atual.

10 — Os elementos constantes dos n.os 1 a 5 são objeto de Regulamento de Execução da Comissão Europeia.

Artigo 20.º

Notificação voluntária de incidentes

1 — Sem prejuízo da obrigação de notificação de incidentes prevista na presente lei, quaisquer entidades podem notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados.

2 — No tratamento das notificações voluntárias, aplica-se o disposto no artigo 17.º, com as necessárias adaptações.

3 — A notificação voluntária não pode dar origem à imposição à entidade notificante de obrigações às quais esta não teria sido sujeita se não tivesse procedido a essa notificação.

CAPÍTULO IV

Fiscalização e sanções

Artigo 21.º

Competências de fiscalização e sancionatórias

As competências de fiscalização e de aplicação das sanções previstas na presente lei cabem ao Centro Nacional de Cibersegurança.

Artigo 22.º

Contraordenações

As infrações ao disposto na presente lei constituem contraordenações, nos termos dos artigos seguintes.

Artigo 23.º

Infrações muito graves

1 — Constituem infrações muito graves:

a) O incumprimento da obrigação de implementar requisitos de segurança tal como previsto nos artigos 14.º, 16.º e 18.º;

b) O incumprimento de instruções de cibersegurança emitidas pelo Centro Nacional de Cibersegurança tal como previsto no n.º 5 do artigo 7.º

2 — As contraordenações referidas no número anterior são punidas com coima de € 5000 a € 25 000, tratando-se de uma pessoa singular, e de € 10 000 a € 50 000, no caso de se tratar de uma pessoa coletiva.

Artigo 24.º

Infrações graves

1 — Constituem infrações graves:

a) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança dos incidentes tal como previsto nos artigos 15.º, 17.º e 19.º;

b) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança do exercício de atividade no setor das infraestruturas digitais tal como previsto no n.º 3 do artigo 29.º;

c) O incumprimento da obrigação de notificar o Centro Nacional de Cibersegurança da identificação como prestador de serviços digitais tal como previsto no artigo 30.º

2 — As contraordenações referidas no número anterior são punidas com coima de € 1000 a € 3000, tratando-se de uma pessoa singular, e de € 3000 a € 9000, no caso de se tratar de uma pessoa coletiva.

Artigo 25.º

Negligência

A negligência é punível, sendo os limites mínimos e máximos das coimas reduzidos a metade.

Artigo 26.º

Instrução dos processos de contraordenação e aplicação de sanções

Compete ao Centro Nacional de Cibersegurança instruir os processos de contraordenação e ao respetivo dirigente máximo a aplicação das coimas.

Artigo 27.º

Produto das coimas

O produto das coimas reverte em:

a) 60 % para o Estado;
b) 40 % para o Centro Nacional de Cibersegurança.

Artigo 28.º

Regime subsidiário

Em matéria contraordenacional, em tudo o que não estiver previsto na presente lei, aplica-se o disposto no regime geral das contraordenações.

CAPÍTULO V

Disposições finais

Artigo 29.º

Identificação de operadores de serviços essenciais

1 — Para efeito do cumprimento da presente lei, o Centro Nacional de Cibersegurança identifica os operadores de serviços essenciais até 9 de novembro de 2018.

2 — A identificação referida no número anterior é objeto de atualização anual.

3 — As entidades do setor das infraestruturas digitais devem comunicar de imediato ao Centro Nacional de Cibersegurança o exercício da respetiva atividade.

Artigo 30.º

Identificação de prestadores de serviços digitais

1 — Os prestadores de serviços digitais devem comunicar de imediato ao Centro Nacional de Cibersegurança o exercício da respetiva atividade.

2 — O dever de notificação referido no número anterior não é aplicável às micro nem às pequenas empresas, tal

como definidas pelo Decreto-Lei n.º 372/2007, de 6 de novembro, na sua redação atual.

Artigo 31.º

Legislação complementar

1 — Os requisitos de segurança previstos no n.º 1 do artigo 14.º e no n.º 1 do artigo 16.º são definidos em legislação própria no prazo de 150 dias após a entrada em vigor da presente lei.

2 — Os requisitos de notificação de incidentes previstos no n.º 1 do artigo 15.º, no n.º 1 do artigo 17.º e no n.º 1 do artigo 19.º são definidos em legislação própria no prazo de 150 dias após a entrada em vigor da presente lei.

Artigo 32.º

Norma revogatória

É revogada a Resolução do Conselho de Ministros n.º 115/2017, de 24 de agosto.

Artigo 33.º

Entrada em vigor e produção de efeitos

1 — A presente lei entra em vigor no dia seguinte ao da sua publicação.

2 — Sem prejuízo do disposto no número anterior, os regimes decorrentes dos artigos 14.º a 27.º produzem efeitos seis meses após a entrada em vigor da presente lei.

Aprovada em 18 de julho de 2018.

O Presidente da Assembleia da República, *Eduardo Ferro Rodrigues.*

Promulgada em 1 de agosto de 2018.

Publique-se.

O Presidente da República, Marcelo Rebelo de Sousa.

Referendada em 6 de agosto de 2018.

O Primeiro-Ministro, *António Luís Santos da Costa.*

ANEXO

(a que se refere o artigo 10.º)

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais

Setor	Subsetor	Tipo de entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.
Transportes	Transporte aéreo	Transportadoras aéreas. Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos. Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
	Transporte ferroviário	Gestores de infraestruturas. Empresas ferroviárias incluindo os operadores de instalações de serviço.
	Transporte marítimo e por vias navegáveis interiores.	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias. Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos. Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias. Operadores de sistemas de transporte inteligentes.
Bancário	—	Instituições de crédito.
Infraestruturas do mercado financeiro	—	Operadores de plataformas de negociação. Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde.	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável.	—	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
Infraestruturas digitais	—	Pontos de troca de tráfego. Prestadores de serviços de Sistema de Nomes de Domínio (DNS). Registos de nomes de domínio de topo.