

de palavra passe que identifique os postos de trabalho, a pessoa que acede à informação, a hora e o tempo de acesso.

### Artigo 12.º

#### Certidão do registo de infrações do condutor e da pontuação dos títulos de condução

1 — A certidão do registo de infrações do condutor e do número de pontos associados ao título de condução é emitida pela ANSR, preferencialmente por meio eletrónico, a requerimento do titular, podendo ser disponibilizada *online* mediante a introdução de um código de validação facultado para o efeito.

2 — [Revogado].

3 — O respetivo serviço emissor deve manter organizado o registo de todas as certidões emitidas nos três meses imediatamente anteriores, por forma a possibilitar a correção ou retificação de certidões emitidas ou a atender a reclamações por eventuais extravios.

4 — [Revogado].

5 — As certidões são devidamente autenticadas pela entidade onde se processa a emissão, não sendo válidas as que apresentem emendas, rasuras ou entrelinhas.

6 — As certidões são válidas por três meses a contar da data da sua emissão.

### Artigo 13.º

#### Segurança da informação

1 — Tendo em vista a segurança da informação, cabe ao responsável pela base de dados a que se refere o presente diploma garantir a observação das seguintes regras:

a) A entrada nas instalações utilizadas para tratamento de dados pessoais é objeto de controlo, a fim de impedir o acesso de qualquer pessoa não autorizada;

b) Os suportes de dados são objeto de controlo a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa não autorizada;

c) A inserção de dados é objeto de controlo para impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizada de dados pessoais;

d) Os sistemas de tratamento automatizado de dados são objeto de controlo para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;

e) O acesso aos dados é objeto de controlo para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;

f) A transmissão dos dados é objeto de controlo para garantir que a sua utilização seja limitada às entidades autorizadas;

g) A introdução, consulta, alteração ou eliminação de dados pessoais nos sistemas de tratamento automatizado é objeto de controlo, de forma a verificar-se quais os dados introduzidos, consultados, alterados ou eliminados, quando e por quem, mantendo-se o registo dessas operações por um período de quatro anos;

h) O transporte de suportes de dados é objeto de controlo para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.

2 — O uso indevido da informação disponível nas bases de dados do RIC é punido nos termos previstos na Lei n.º 67/98, de 26 de outubro.

## JUSTIÇA

### Decreto-Lei n.º 81/2016

de 28 de novembro

O desenvolvimento de uma estratégia adequada de combate ao cibercrime pressupõe que as entidades responsáveis pela respetiva prevenção e repressão detenham informação (*cyber-intelligence*) em tempo útil que possibilite, não só a deteção precoce de ataques digitais, mas também a compreensão da intenção criminosa associada ao uso, à comercialização e à disseminação de programas maliciosos.

O estabelecimento de uma política criminal coerente para o cibercrime deve assentar em parâmetros flexíveis e adaptáveis a longo prazo mas que, simultaneamente, possibilitem uma atuação imediata sem colidir com as demais linhas de orientação fixadas na Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, permitindo, deste modo, o desenvolvimento da necessária articulação entre a capacidade nacional de resposta a incidentes e o combate ao Cibercrime, expresso no «Eixo 2».

Daí que se torne necessário a Polícia Judiciária reforçar o ajustamento com as estruturas europeias e internacionais de informação e contrainformação criminal (v.g., a EURO-POL e a INTERPOL), tendo em vista a luta eficaz contra o cibercrime assente na recolha e partilha de informações criminais e criminógenas, na constituição de equipas internacionais que permitam respostas articuladas entre Polícias e representantes das Magistraturas e na realização de operações policiais transnacionais.

Urge, pois, implementar uma unidade operacional especializada na Polícia Judiciária, típica de uma Polícia Científica, que permita alcançar a necessária resposta estrutural, preventiva e repressiva ao fenómeno do cibercrime e do ciberterrorismo, e que é inspirada no modelo adotado pelo EC3 (*European Cybercrime Center*) da EUROPOL, cujos pontos focais são o abuso sexual de crianças através da Internet, a fraude com os cartões e outros meios de pagamento eletrónico e virtuais, a criminalidade informática pura (os crimes previstos na Lei n.º 109/2009, de 15 de setembro) e a criminalidade praticada com recurso a meios informáticos.

A Lei n.º 103/2015, de 24 de agosto criou, na Polícia Judiciária, uma unidade nacional, a Unidade Nacional de Investigação da Criminalidade Informática, cujas competências internas nunca foram estabelecidas, e introduziu a correspondente alteração na Lei n.º 37/2008, de 6 de agosto.

O presente decreto-lei não atribuindo, como não poderia atribuir, novas e diferentes competências à Polícia Judiciária, disciplina no plano interno desta Polícia as competências das respetivas unidades, procedendo a uma redistribuição e concentrando numa única estrutura atribuições hoje dispersas por diferentes unidades.

Optou-se por adequar a nomenclatura daquela Unidade e dotá-la de um núcleo de competências adaptadas às orientações traçadas pelas suas congéneres europeias no EC3.

Assim, a Unidade então criada será substituída por uma nova que se designará — à semelhança da congénere da EUROPOL — EC3 — por Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T).

Preservando o princípio da coesão funcional, o presente decreto-lei visa não só modernizar e adequar a estrutura orgânica da Polícia Judiciária a esta nova Unidade, mas também adaptar as competências da Unidade Nacional Contra-Terrorismo às especificidades do ciberespaço.

Para o efeito, cumpre alterar a Lei n.º 37/2008, de 6 de agosto, que define a orgânica da Polícia Judiciária, o Decreto-Lei n.º 42/2009, de 12 de fevereiro, que estabelece as competências das unidades da Polícia Judiciária e o regime remuneratório dos seus dirigentes, e a Portaria n.º 304/2009, de 25 de março, que estabelece os lugares de direção superior e intermédia da Polícia Judiciária.

Foram ouvidos o Conselho Superior da Magistratura, o Conselho Superior do Ministério Público, a Comissão Nacional de Proteção de Dados e a Associação Sindical dos Funcionários de Investigação Criminal.

Assim:

Nos termos da alínea *a*) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

#### Artigo 1.º

##### Objeto

1 — É criada, na estrutura orgânica da Polícia Judiciária, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, designada abreviadamente pela sigla UNC3T.

2 — A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica substitui a Unidade Nacional da Investigação da Criminalidade Informática, a qual é extinta.

#### Artigo 2.º

##### Alteração à Lei n.º 37/2008, de 6 de agosto

O artigo 28.º da Lei n.º 37/2008, de 6 de agosto, alterada pela Lei n.º 26/2010, de 30 de agosto, e pela Lei n.º 103/2015, de 24 de agosto, passa a ter a seguinte redação:

#### «Artigo 28.º

[...]

1 — [...]:

*a*) [...]

*b*) [...]

*c*) [...]

*d*) A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

2 — [...].»

#### Artigo 3.º

##### Alteração ao Decreto-Lei n.º 42/2009, de 12 de fevereiro

Os artigos 2.º, 7.º e 10.º do Decreto-Lei n.º 42/2009, de 12 de fevereiro, passam a ter a seguinte redação:

#### «Artigo 2.º

[...]

1 — [...]:

*a*) [...]

*b*) [...]:

*i*) [...]

*ii*) [...]

*iii*) [...]

*iv*) A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica;

*c*) [...]

*d*) [...]

*e*) [...]

*f*) [...]

*g*) [...].

2 — [...].

3 — [...].

4 — [...].

5 — [...].

6 — [...].

7 — [...].

#### Artigo 7.º

[...]

1 — [...]:

*a*) Organizações terroristas, terrorismo e o seu financiamento, incluindo os atos praticados com recurso, através de ou contra sistema informático;

*b*) [...]

*c*) [...]

*d*) [...]

*e*) [...]

*f*) [...].

2 — [...].

#### Artigo 10.º

[...]

1 — [...].

2 — A UNCT e a UNC3T dispõem de extensões nas unidades territoriais localizadas fora da respetiva sede, ficando organicamente integradas nestas unidades.

3 — [...].»

#### Artigo 4.º

##### Aditamento ao Decreto-Lei n.º 42/2009, de 12 de fevereiro

É aditado ao Decreto-Lei n.º 42/2009, de 12 de fevereiro, o artigo 9.º-A, com a seguinte redação:

#### «Artigo 9.º-A

##### Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica

1 — A Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, designada abreviadamente pela sigla UNC3T, tem as seguintes competências:

*a*) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na Lei n.º 109/2009, de 15 de setembro;

*b*) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, designadamente:

*i*) Na Lei de Proteção dos Dados Pessoais;

*ii*) No Código dos Direitos de Autor e Direitos Conexos, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços;

*c*) Prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes:

*i*) Contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático;

*ii*) De devassa por meio da informática;

- iii) De burla informática e nas comunicações;
- iv) Relativos à interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais;
- v) De espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente.

2 — A UNC3T assegura, no âmbito da cooperação internacional, o ponto de contacto operacional permanente previsto no artigo 21.º da Lei n.º 109/2009, de 15 de setembro.

3 — A UNC3T colabora e apoia de forma direta as ações de prevenção, deteção e mitigação desenvolvidas pelas entidades nacionais com competências definidas por lei para a segurança nacional do ciberespaço.

4 — Cabe ainda à UNC3T:

a) Elaborar e manter atualizado o Plano Nacional da Polícia Judiciária para a Prevenção e o Combate ao Cibercrime, nomeadamente, em articulação com o Centro Nacional de Cibersegurança;

b) Celebrar protocolos de colaboração técnica e científica com entidades públicas e privadas, nacionais ou estrangeiras, mediante prévia aprovação da direção nacional;

c) Assegurar o regular funcionamento de um grupo consultivo informal para debate e aconselhamento estratégico, formativo, jurídico, técnico e científico de questões relacionadas com o cibercrime, com a criminalidade tecnológica e a cibersegurança;

d) Assegurar a colaboração e participação direta na formação inicial e contínua sobre cibercrime aos quadros do pessoal de investigação criminal e de apoio da Polícia Judiciária, designadamente, nas áreas da segurança da informação e da cibersegurança.

5 — Na UNC3T e sob a dependência da sua direção é criada uma equipa técnica e de investigação digital com as seguintes funções:

a) Otimizar e gerir as infraestruturas e meios tecnológicos atribuídos à Unidade;

b) Apoiar e assessorar nos planos técnico, tecnológico e jurídico, o pessoal de investigação criminal nas suas investigações;

c) Testar e desenvolver ferramentas específicas para a investigação do cibercrime, da criminalidade tecnológica e da decifragem de dados;

d) Recolher, tratar e difundir dados relativos a *ciber-intelligence* para apoio às investigações, à cooperação policial internacional e à prevenção de atos de cibercrime;

e) Desenvolver ações de contrainformação criminal;

f) Dar apoio em ações de caráter técnico para recolha de prova digital, nomeadamente, ações encobertas e interceção de dados;

g) Apoiar investigações que exijam conhecimentos técnicos especializados, nomeadamente, redes de anonimização, mercados virtuais, moedas virtuais, análise de programas maliciosos.

6 — A UNC3T goza de autonomia técnica e científica.»

#### Artigo 5.º

##### Alteração à Portaria n.º 304/2009, de 25 de março

O mapa com o número de lugares de direção superior e intermédia da Polícia Judiciária, constante do anexo à

Portaria n.º 304/2009, de 25 de março, passa a ter a redação constante do anexo ao presente decreto-lei, do qual faz parte integrante.

#### Artigo 6.º

##### Mapa de pessoal

O mapa de pessoal da Polícia Judiciária é alterado de modo a prever que o preenchimento de postos de trabalho de que a UNC3T carece para o desenvolvimento da sua atividade é feito com pessoal de outras unidades orgânicas, nomeadamente por elementos da 8.ª Secção da Diretoria de Lisboa e Vale do Tejo, com perfil de competências adequado.

#### Artigo 7.º

##### Entrada em vigor

O presente decreto-lei entra em vigor no dia seguinte ao da sua publicação.

Visto e aprovado em Conselho de Ministros de 6 de outubro de 2016. — *António Luís Santos da Costa* — *Mário José Gomes de Freitas Centeno* — *José Alberto de Azevedo Ferreira Lopes* — *Maria Constança Dias Urbano de Sousa* — *Helena Maria Mesquita Ribeiro*.

Promulgado em 17 de novembro de 2016.

Publique-se.

O Presidente da República, MARCELO REBELO DE SOUSA.

Referendado em 23 de novembro de 2016.

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

#### ANEXO

(a que se refere o artigo 5.º)

#### Anexo à Portaria n.º 304/2009, de 25 de março

##### Mapa de pessoal dirigente

Designação de cargos dirigentes	Número de lugares
Diretor nacional	...
Diretor nacional-adjunto	...
Diretor de unidade nacional	4
Diretor de unidade territorial	...
Subdiretor de unidade territorial	...
Diretor da Escola de Polícia Judiciária	...
Diretor da Unidade de Prevenção e Apoio Tecnológico	...
Diretor da Unidade de Informação Financeira	...
Diretor da Unidade de Planeamento, Assessoria Técnica e Documentação	...
Diretor de Unidade de Apoio à Investigação	...
Diretor da Unidade de Suporte	...
Chefe de área	...

## TRABALHO, SOLIDARIEDADE E SEGURANÇA SOCIAL

### Portaria n.º 295/2016

de 28 de novembro

O Decreto-Lei n.º 165-A/2013, de 23 de dezembro, criou o Fundo de Reestruturação do Setor Solidário (FRSS), o