

# Jornal Oficial da União Europeia

# L 351 I



Edição em língua  
portuguesa

## Legislação

63.º ano

22 de outubro de 2020

Índice

II *Atos não legislativos*

REGULAMENTOS

- ★ Regulamento de Execução (UE) 2020/1536 do Conselho, de 22 de outubro de 2020, que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros ..... 1

DECISÕES

- ★ Decisão (PESC) 2020/1537 do Conselho, de 22 de outubro de 2020, que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros ..... 5

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.



## II

(Atos não legislativos)

## REGULAMENTOS

## REGULAMENTO DE EXECUÇÃO (UE) 2020/1536 DO CONSELHO

de 22 de outubro de 2020

**que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros**

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros <sup>(1)</sup>, nomeadamente o artigo 13.º, n.º 1,

Tendo em conta a proposta do alto representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 17 de maio de 2019, o Conselho adotou o Regulamento (UE) 2019/796.
- (2) As medidas restritivas específicas contra os ciberataques com efeitos significativos que constituem uma ameaça externa para a União ou para os seus Estados-Membros integram as medidas incluídas no quadro da União para uma resposta diplomática conjunta às ciberatividades maliciosas (conjunto de instrumentos de ciberdiplomacia), e são um instrumento vital para dissuadir e dar resposta a tais atividades.
- (3) A fim de prevenir, desencorajar, dissuadir e responder aos continuados e crescentes casos de comportamentos maliciosos no ciberespaço, duas pessoas singulares e um organismo deverão ser incluídos na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo do Regulamento (UE) 2019/796. Essas pessoas e esse organismo são responsáveis por ciberataques ou participaram em ciberataques com efeitos significativos que constituem uma ameaça externa para a União ou para os seus Estados-Membros, nomeadamente o ciberataque de abril e maio de 2015 contra o Parlamento Federal alemão (*Deutscher Bundestag*).
- (4) Por conseguinte, o anexo I do Regulamento (UE) 2019/796 deverá ser alterado em conformidade,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O anexo I do Regulamento (UE) 2019/796 é alterado em conformidade com o anexo da presente decisão.

<sup>(1)</sup> JOL 129 I de 17.5.2019, p. 1.

*Artigo 2.º*

O presente regulamento entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 22 de outubro de 2020.

*Pelo Conselho*  
*O Presidente*  
M. ROTH

---

## ANEXO

As seguintes entradas são aditadas à lista de pessoas singulares e coletivas, entidades e organismos constante do anexo I do Regulamento (UE) 2019/796:

## A. Pessoas singulares

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«7.	Dmitry Sergeevich BADIN	<p>Дмитрий Сергеевич БАДИН</p> <p>Data de nascimento: 15 de novembro de 1990</p> <p>Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia)</p> <p>Nacionalidade: russa</p> <p>Sexo: masculino</p>	<p>Dmitry Badin participou num ciberataque com efeitos importantes contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>).</p> <p>Enquanto agente dos serviços de informação militares do 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), Dmitry Badin fez parte de uma equipa de agentes dos serviços de informações militares russos que lançaram um ataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) em abril e maio de 2015. O referido ciberataque visou o sistema informático do Parlamento Federal alemão e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020
8.	Igor Olegovich KOSTYUKOV	<p>Игорь Олегович КОСТИУКОВ</p> <p>Data de nascimento: 21 de fevereiro de 1961</p> <p>Nacionalidade: russa</p> <p>Sexo: masculino</p>	<p>Igor Kostyukov é o atual chefe da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), tendo anteriormente ocupado o cargo de primeiro chefe adjunto. Uma das unidades sob o seu comando é o 85.º Centro Principal de Serviços Especiais (GTsSS), também chamada “unidade militar 26165” (outros nomes por que é conhecida no setor da cibersegurança: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” e “Strontium”).</p> <p>No exercício desse cargo, Igor Kostyukov é responsável por ciberataques lançados pelo GTsSS, incluindo ataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros.</p> <p>Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de ciberataque destinado a piratear a rede Wi-Fi da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos.</p> <p>O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020»

B. Pessoas coletivas, entidades e organismos

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«4.	85 <sup>th</sup> Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia]	Endereço: Komsomol'skiy Prospekt, 20, Moscovo, 119146, Federação da Rússia	<p>O 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), também chamada “unidade militar 26165” (outros nomes por que é conhecida no setor da cibersegurança: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” e “Strontium”), é responsável por ciberataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros.</p> <p>Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de ciberataque destinado a piratear a rede Wi-Fi da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos.</p> <p>O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020»

# DECISÕES

## DECISÃO (PESC) 2020/1537 DO CONSELHO

de 22 de outubro de 2020

### que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 29.º,

Tendo em conta a proposta do alto representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 17 de maio de 2019, o Conselho adotou a Decisão (PESC) 2019/797 <sup>(1)</sup>.
- (2) As medidas restritivas específicas contra os ciberataques com efeitos significativos que constituem uma ameaça externa para a União ou para os seus Estados-Membros integram as medidas incluídas no quadro da União para uma resposta diplomática conjunta às ciberatividades maliciosas (conjunto de instrumentos de ciberdiplomacia), e são um instrumento vital para dissuadir e dar resposta a tais atividades.
- (3) A fim de prevenir, desencorajar, dissuadir e responder aos continuados e crescentes casos de comportamentos maliciosos no ciberespaço, duas pessoas singulares e um organismo deverão ser incluídos na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo da Decisão (PESC) 2019/797. Essas pessoas e esse organismo são responsáveis por ciberataques ou participaram em ciberataques com efeitos significativos que constituem uma ameaça externa para a União ou para os seus Estados-Membros, nomeadamente o ciberataque de abril e maio de 2015 contra o Parlamento Federal alemão (*Deutscher Bundestag*).
- (4) Por conseguinte, a Decisão (PESC) 2019/797 deverá ser alterada em conformidade,

ADOTOU A PRESENTE DECISÃO:

#### Artigo 1.º

O anexo da Decisão (PESC) 2019/797 é alterado em conformidade com o anexo da presente decisão.

#### Artigo 2.º

A presente decisão entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 22 de outubro de 2020.

*Pelo Conselho*  
*O Presidente*  
M. ROTH

---

<sup>(1)</sup> Decisão (PESC) 2019/797 do Conselho, de 17 de maio de 2019, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 129 I de 17.5.2019, p. 13).

## ANEXO

As seguintes entradas são aditadas à lista de pessoas singulares e coletivas, entidades e organismos constante do anexo da Decisão (PESC) 2019/797:

## A. Pessoas singulares

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«7.	Dmitry Sergeyevich BADIN	<p>Дмитрий Сергеевич БАДИН</p> <p>Data de nascimento: 15 de novembro de 1990</p> <p>Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia)</p> <p>Nacionalidade: russa</p> <p>Sexo: masculino</p>	<p>Dmitry Badin participou num ciberataque com efeitos importantes contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>).</p> <p>Enquanto agente dos serviços de informação militares do 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), Dmitry Badin fez parte de uma equipa de agentes dos serviços de informações militares russos que lançaram um ataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) em abril e maio de 2015. O referido ciberataque visou o sistema informático do Parlamento Federal alemão e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020
8.	Igor Olegovich KOSTYUKOV	<p>Игорь Олегович КОСТИУКОВ</p> <p>Data de nascimento: 21 de fevereiro de 1961</p> <p>Nacionalidade: russa</p> <p>Sexo: masculino</p>	<p>Igor Kostyukov é o atual chefe da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), tendo anteriormente ocupado o cargo de primeiro chefe adjunto. Uma das unidades sob o seu comando é o 85.º Centro Principal de Serviços Especiais (GTsSS), também chamada “unidade militar 26165” (outros nomes por que é conhecida no setor da cibersegurança: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” e “Strontium”).</p> <p>No exercício desse cargo, Igor Kostyukov é responsável por ciberataques lançados pelo GTsSS, incluindo ataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros.</p> <p>Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de ciberataque destinado a piratear a rede Wi-Fi da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos.</p> <p>O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020»



B. Pessoas coletivas, entidades e organismos

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«4.	85 <sup>th</sup> Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia]	Endereço: Komsomol'skiy Prospekt, 20, Moscovo, 119146, Federação da Rússia	<p>O 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), também chamada “unidade militar 26165” (outros nomes por que é conhecida no setor da cibersegurança: “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” e “Strontium”), é responsável por cibertaquês com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros.</p> <p>Mais especificamente, agentes de informações militares do GTsSS participaram no cibertaque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de cibertaque destinado a piratear a rede <i>Wi-Fi</i> da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos.</p> <p>O cibertaque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.</p>	22.10.2020»



ISSN 1977-0774 (edição eletrónica)  
ISSN 1725-2601 (edição em papel)