RECOMENDAÇÕES

RECOMENDAÇÃO (UE) 2019/534 DA COMISSÃO

de 26 de março de 2019

Cibersegurança das redes 5G

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

(1) A Comissão reconheceu que a implantação da 5.ª geração (5G) das tecnologias de rede é um elemento facilitador essencial para os futuros serviços digitais e constitui uma prioridade da Estratégia para o Mercado Único Digital. A Comissão adotou o Plano de Ação 5G a fim de garantir que a União disponha das infraestruturas de conectividade necessárias para a sua transformação digital a partir de 2020 ([1]).

(2) As redes 5G assentarão na atual 4.ª geração (4G) das tecnologias de rede, oferecendo novas capacidades de serviços e tornando-se a infraestrutura central e o elemento facilitador de setores substanciais da economia da União. Uma vez implantadas, as redes 5G constituirão a espinha dorsal de uma vasta gama de serviços essenciais ao funcionamento do mercado interno e à manutenção e funcionamento de funções vitais da sociedade e da economia — energia, transportes, banca e saúde, bem como sistemas de controlo industriais. Para a organização dos processos democráticos, como eleições, recorrer-se-á também cada vez mais às infraestruturas digitais e às redes 5G.

(3) A dependência de muitos serviços críticos em relação às redes 5G faria com que as consequências de perturbações sistémicas e generalizadas pudessem ser particularmente graves. Por conseguinte, garantir a cibersegurança das redes 5G é uma questão de importância estratégica para a União, num momento em que os ciberataques estão a aumentar e são mais sofisticados do que nunca.

(4) A natureza interligada e transnacional das infraestruturas subjacentes ao ecossistema digital e a natureza transfronteiras das ameaças envolvidas implicam que eventuais vulnerabilidades e/ou incidentes de cibersegurança significativos nas redes 5G verificados num Estado-Membro afetariam a União no seu conjunto. É por essa razão que devem ser estabelecidas medidas para garantir um elevado nível comum de cibersegurança das redes 5G.

(5) A necessidade de ação a nível da União foi confirmada pelos Estados-Membros. Nas suas conclusões de 21 de março de 2019, o Conselho Europeu aguarda com expectativa uma recomendação da Comissão relativa a uma abordagem concertada em matéria de segurança das redes 5G ([2]).

(6) Garantir a soberania europeia, no pleno respeito dos valores de abertura e tolerância da Europa, deve constituir um objetivo fundamental ([3]). O investimento estrangeiro em setores estratégicos, a aquisição de ativos, tecnologias e infraestruturas de importância crítica na União e o fornecimento de equipamentos críticos podem também representar riscos para a segurança da União.

(7) A cibersegurança das redes 5G é fundamental para assegurar a autonomia estratégica da União, conforme reconhecido na Comunicação Conjunta «UE-China – Uma perspetiva estratégica» ([4])

(8) A resolução do Parlamento Europeu sobre as ameaças para a segurança resultantes do reforço da presença tecnológica chinesa na UE apela também a que a Comissão e os Estados-Membros tomem medidas a nível da União ([5]).

(9) A presente recomendação aborda os riscos de cibersegurança nas redes 5G estabelecendo orientações sobre a análise de risco e as medidas de gestão adequadas a nível nacional, sobre o desenvolvimento de uma avaliação coordenada dos riscos a nível da UE e sobre o estabelecimento de um processo para desenvolver um conjunto de instrumentos comuns que permitam adotar as medidas de gestão dos riscos mais eficientes.

(10) A União dispõe de um quadro legislativo sólido para proteger as redes de comunicações eletrónicas.

([1]) COM(2016) 588 final.
([2]) Conclusões do Conselho Europeu de 21 e 22 de Março de 2019.
([3]) Estado da União 2018 — «A hora da soberania europeia», 12 de setembro de 2018.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//EN.

(11) O quadro da União no domínio das comunicações eletrónicas ([6]) promove a concorrência, o mercado interno e os interesses dos utilizadores finais e com o Código Europeu das Comunicações Eletrónicas ([7]) visa atingir um objetivo de conectividade adicional, articulado em termos de resultados: acesso generalizado e adoção de conectividade fixa e móvel de muito elevada capacidade para todos os cidadãos e empresas da União, salvaguardando simultaneamente os interesses dos cidadãos. A Diretiva 2002/21/CE estabelece que os Estados-Membros devem assegurar a manutenção da integridade e da segurança das redes de comunicações públicas, com obrigações destinadas a assegurar que as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público tomem medidas técnicas e organizativas para gerir adequadamente os riscos para a segurança das redes e serviços. Estabelece também que as autoridades reguladoras nacionais competentes devem ter poderes, incluindo o poder de emitir instruções vinculativas, para assegurar o cumprimento dessas obrigações.

(12) Além disso, a Diretiva 2002/20/CE do Parlamento Europeu e do Conselho ([8]) permite aos Estados-Membros associar à autorização geral certas condições relativas à segurança das redes públicas contra o acesso não autorizado, para proteger a confidencialidade das comunicações em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([9]).

(13) Com vista a apoiar o cumprimento destas obrigações, a União criou uma série de organismos de cooperação. A Agência para a Segurança das Redes e da Informação (ENISA), a Comissão, os Estados-Membros e as autoridades reguladoras nacionais elaboraram orientações técnicas dirigidas às autoridades reguladoras nacionais em matéria de comunicação de incidentes, medidas de segurança e ameaças a bens ([10]). O Grupo de Cooperação instituído pela Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([11]) («o Grupo de Cooperação») reúne as autoridades competentes a fim de apoiar e facilitar a cooperação, nomeadamente fornecendo orientações estratégicas para as atividades da Rede de Equipas de Resposta a Incidentes de Segurança Informática, o que, a nível técnico, facilita a cooperação operacional.

(14) O futuro quadro europeu de certificação da cibersegurança ([12]) deverá constituir um instrumento de apoio essencial para promover níveis coerentes de segurança. Deverá permitir o desenvolvimento de sistemas de certificação da cibersegurança para dar resposta às necessidades dos utilizadores de equipamentos e programas informáticos relacionados com a G5. Devido à importância crítica destas infraestruturas, deverá ser dada prioridade imediata à elaboração de sistemas europeus de certificação da cibersegurança relevantes para os produtos, os serviços ou os processos das tecnologias da informação e das comunicações utilizados nas redes 5G. Os Estados-Membros e os intervenientes no mercado devem participar ativamente no desenvolvimento desses sistemas de certificação, nomeadamente apoiando a definição de perfis de proteção específicos para as redes 5G.

(15) Na ausência de legislação harmonizada da União, os Estados-Membros podem especificar, por meio de regulamentos técnicos nacionais, adotados em conformidade com o direito da União, que deve ser obrigatório um sistema europeu de certificação da cibersegurança. Os Estados-Membros também recorrem a sistemas europeus de certificação da cibersegurança no contexto de contratos públicos e no âmbito da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho ([13]) e podem apoiar o desenvolvimento de mecanismos de assistência — como, por exemplo, uma plataforma de assistência — para a aquisição de soluções de cibersegurança por parte de adquirentes públicos.

(16) Um elevado nível de proteção dos dados e da privacidade constitui um elemento importante para garantir a segurança das redes 5G. Foram igualmente definidas regras a nível da União destinadas a garantir a segurança do tratamento de dados pessoais, nomeadamente nas comunicações eletrónicas. O Regulamento Geral de Proteção de Dados ([14]) prevê que o tratamento dos dados pessoais deve obrigatoriamente garantir a sua segurança, designadamente para impedir o acesso e a utilização não autorizados a dados pessoais e a equipamentos utilizados para o tratamento dos dados. A diretiva relativa à privacidade e às comunicações

([6]) Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro) (JO L 108 de 24.4.2002, p. 33) e Diretivas Específicas.

([7]) Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (JO L 321 de 17.12.2018, p. 36).

([8]) Diretiva 2002/20/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa à autorização de redes e serviços de comunicações eletrónicas (Diretiva Autorização) (JO L 108 de 24.4.2002, p. 21).

([9]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Directiva relativa à privacidade e às comunicações electrónicas) (JO L 201 de 31.7.2002, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) 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 (JO L 194 de 19.7.2016, p. 1).

([12]) Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.o 526/2013 («Regulamento Cibersegurança») [COM(2017) 0477 final — 2017/0225 (COD)].

([13]) Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

([14]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

eletrónicas estabelece regras específicas sobre a proteção da confidencialidade das comunicações e do equipamento terminal dos utilizadores finais. Impõe também obrigações aos prestadores de serviços no sentido de tomarem medidas técnicas e organizativas adequadas para salvaguardar a segurança dos seus serviços.

(17) A União adotou também um instrumento que protegerá infraestruturas e tecnologias de importância crítica, como as utilizadas nas comunicações, permitindo aos Estados-Membros escrutinar os investimentos diretos estrangeiros por razões de segurança ou de ordem pública e criando um mecanismo de cooperação no âmbito do qual os Estados-Membros e a Comissão poderão trocar informações e expressar as suas preocupações quanto a determinados investimentos ([15]).

(18) Os Estados-Membros e os operadores estão atualmente a tomar medidas preparatórias importantes com vista a permitir a implantação em grande escala das redes 5G. Vários Estados-Membros manifestaram a sua preocupação quanto aos potenciais riscos de segurança relacionados com as redes 5G no contexto da execução de procedimentos para a concessão de direitos de utilização nas faixas do espetro de radiofrequências designadas para as redes 5G ([16]), tendo estudado medidas para enfrentar esses riscos.

(19) Na abordagem dos riscos de cibersegurança nas redes 5G deve ter-se em conta fatores técnicos e fatores de outra ordem. Os fatores técnicos podem incluir vulnerabilidades de cibersegurança que possam ser exploradas para obter acesso não autorizado a informações (ciberespionagem, seja por razões económicas ou políticas) ou para outros fins mal-intencionados (ciberataques destinados a perturbar ou destruir sistemas e dados). Alguns dos aspetos importantes a considerar devem ser a necessidade de proteger as redes ao longo de todo o seu ciclo de vida e a necessidade de abranger todos os equipamentos relevantes, nomeadamente nas fases de conceção, desenvolvimento, concurso para aquisição, implantação, funcionamento e manutenção das redes 5G.

(20) Outros fatores podem incluir requisitos regulamentares ou de outra ordem, impostos aos fornecedores de equipamentos de tecnologias da informação e das comunicações. Uma avaliação da importância desses fatores deveria ter em conta, *inter alia*, o risco global de influência de um país terceiro, nomeadamente em relação ao seu modelo de governação, a ausência de acordos de cooperação em matéria de segurança, ou de convénios similares, como decisões de adequação, em matéria de proteção de dados entre a União e o país terceiro em causa ou, se este país é parte em acordos multilaterais, internacionais ou bilaterais sobre cibersegurança, a luta contra a cibercriminalidade ou a proteção de dados.

(21) Dado tratar-se de um passo importante no desenvolvimento de uma abordagem da União em matéria de cibersegurança das redes 5G, deve ser realizada e concluída uma avaliação dos riscos a nível nacional. Tal ajudaria os Estados-Membros a adaptar as medidas nacionais em matéria de requisitos de segurança e de gestão de riscos aos resultados desta avaliação.

(22) A coordenação é um elemento importante a desenvolver a fim de garantir a eficácia das medidas destinadas a enfrentar estas ameaças à cibersegurança, medidas que são essenciais para o bom funcionamento do mercado interno e para a proteção dos dados pessoais e da privacidade.

(23) As avaliações nacionais dos riscos devem constituir a base de uma avaliação coordenada dos riscos a nível da União, composta pelo levantamento do panorama das ameaças e por uma revisão conjunta a realizar pelos Estados-Membros, com o apoio da Comissão e em conjunto com a Agência Europeia para a Cibersegurança (ENISA).

(24) Tendo em conta as avaliações dos riscos a nível nacional e da União, o Grupo de Cooperação deve criar um conjunto de instrumentos que permita identificar os tipos de riscos de cibersegurança e as medidas possíveis para reduzir os riscos em domínios como a certificação, os ensaios e os controlos de acesso. Este grupo deve igualmente identificar possíveis medidas específicas adequadas para enfrentar os riscos recenseados por um ou mais Estados-Membros. O Grupo de Cooperação deve beneficiar do apoio da Agência Europeia para a Cibersegurança (ENISA), da Europol, do Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE) e do Centro de Situação e de Informações da UE. Este conjunto de instrumentos deve servir para aconselhar a Comissão sobre o desenvolvimento de requisitos comuns mínimos que permitam garantir um nível elevado de cibersegurança das redes 5G em toda a União.

(25) Na elaboração das medidas destinadas a fazer face aos riscos de cibersegurança, deve ser tida em conta a promoção da cibersegurança através da diversidade de fornecedores quando da construção de uma rede.

([15]) Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho, de 19 de março de 2019, que estabelece um regime de análise dos investimentos diretos estrangeiros na União (JO L 79I de 21.3.2019, p. 1).

([16]) O procedimento de leilão em, pelo menos, uma faixa do espetro está previsto para 2019 em 11 Estados-Membros: Alemanha, Áustria, Bélgica, Chéquia, França, Grécia, Hungria, Irlanda, Lituânia, Países Baixos, Portugal. Estão previstos mais seis leilões para 2020: Eslováquia, Espanha, Lituânia (frequências diferentes), Malta, Polónia e Reino Unido. *Fonte:* http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) A presente recomendação é aplicável sem prejuízo das competências dos Estados-Membros no que respeita às atividades relacionadas com a segurança pública, a defesa, a segurança nacional e as atividades do Estado em domínios do direito penal, incluindo o direito de os Estados-Membros excluírem certos prestadores de serviços ou fornecedores dos seus mercados por razões de segurança nacional.

ADOTOU A PRESENTE RECOMENDAÇÃO:

I. **OBJETIVOS**

1. A fim de apoiar o desenvolvimento de uma abordagem da União destinada a garantir a cibersegurança das redes 5G, a presente recomendação identifica as ações que devem ser tomadas para permitir:

   a) Aos Estados-Membros avaliar os riscos de cibersegurança que afetam as redes 5G a nível nacional e tomar as medidas de segurança necessárias;

   b) Aos Estados-Membros e às instituições, agências e outros organismos da União desenvolver conjuntamente uma avaliação coordenada dos riscos a nível da União baseada nas avaliações de riscos realizadas a nível nacional.

   c) Ao Grupo de Cooperação, criado ao abrigo da Diretiva (UE) 2016/1148 (Grupo de Cooperação), identificar um possível conjunto de medidas comuns a adotar para atenuar os riscos em matéria de cibersegurança relacionados com as infraestruturas subjacentes ao ecossistema digital, em especial as redes 5G.

II. **DEFINIÇÕES**

2. Para efeitos da presente recomendação, entende-se por:

   a) «Redes 5G»: um conjunto de todos os elementos relevantes da infraestrutura das redes para tecnologias de comunicações móveis e sem fios utilizadas para fins de conectividade e em serviços de valor acrescentado com características de desempenho avançadas, tais como velocidades de débito e capacidade de dados muito elevadas, comunicações de baixa latência, de fiabilidade ultra elevada ou que suportem um grande número de dispositivos conectados. Podem incluir elementos das redes históricas baseados em gerações de tecnologias de comunicações móveis e sem fios anteriores, tais como as tecnologias 4G ou 3G. As redes 5G devem ser entendidas como incluindo todas as partes relevantes da rede.

   b) «Infraestruturas subjacentes ao ecossistema digital»: infraestruturas utilizadas para permitir a digitalização numa vasta gama de aplicações de importância crítica para a economia e a sociedade.

III. **AÇÃO A NÍVEL NACIONAL**

3. Até 30 de junho de 2019, os Estados-Membros devem proceder a uma avaliação dos riscos da infraestrutura de redes 5G, incluindo a identificação dos elementos mais sensíveis relativamente aos quais as violações da segurança podem ter um impacto negativo significativo. Até à mesma data, os Estados-Membros devem também proceder à revisão dos requisitos de segurança e dos métodos de gestão de riscos aplicáveis a nível nacional, a fim de ter em conta as ameaças à cibersegurança suscetíveis de resultar: i) de fatores técnicos, como as características técnicas específicas das redes 5G e ii) de outros fatores, como o quadro jurídico e político a que os fornecedores de equipamentos de tecnologias da informação e das comunicações possam estar sujeitos em países terceiros.

4. Com base nesta revisão e avaliação dos riscos a nível nacional e tendo em conta a ação coordenada em curso a nível da União, os Estados-Membros devem:

   a) Atualizar os requisitos de segurança e os métodos de gestão dos riscos aplicados às redes 5G;

   b) Atualizar as obrigações relevantes impostas às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público nos termos dos artigos 13.º-A e 13.º-B da Diretiva 2002/21/CE;

   c) Associar condições à autorização geral relativas à segurança das redes públicas contra o acesso não autorizado e solicitar compromissos às empresas que participem em procedimentos futuros de concessão de direitos de utilização de radiofrequências nas bandas 5G no que diz respeito ao cumprimento dos requisitos de segurança aplicáveis às redes nos termos da Diretiva 2002/20/CE;

   d) Aplicar outras medidas preventivas destinadas a atenuar os potenciais riscos de cibersegurança.

5. As medidas referidas no ponto 4 devem prever obrigações reforçadas aplicáveis aos fornecedores e operadores no sentido de assegurarem a segurança de partes sensíveis das redes, bem como obrigações, quando adequado, relativas ao fornecimento de informações relevantes às autoridades nacionais competentes sobre as alterações previstas nas redes de comunicações eletrónicas e aos requisitos aplicáveis aos laboratórios nacionais de auditoria/certificação no sentido de procederem a ensaios prévios dos componentes e sistemas de tecnologias da informação específicos para fins de segurança e de integridade.

6. As revisões de segurança conjuntas devem ser realizadas por dois ou mais Estados-Membros, utilizando e partilhando as competências técnicas e os recursos adequados relacionados com as infraestruturas subjacentes ao ecossistema digital e às redes 5G, por exemplo quando uma mesma empresa opera ou constrói infraestruturas de rede em mais do que um Estado-Membro ou quando existem semelhanças importantes nas configurações das redes. A Agência Europeia para a Cibersegurança (ENISA), a Europol e o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE) devem dar prioridade aos pedidos dos Estados-Membros de apoio neste domínio. Os resultados destas revisões devem ser transmitidos ao Grupo de Cooperação e à Rede de Equipas de Resposta a Incidentes de Segurança Informática.

IV. **AÇÃO COORDENADA A NÍVEL DA UNIÃO**

7. A fim de desenvolver uma abordagem comum para enfrentar os riscos de cibersegurança no que diz respeito às redes 5G, os Estados-Membros devem começar a funcionar de acordo com um fluxo específico de trabalho no âmbito do Grupo de Cooperação até 30 de abril de 2019. Quando adequado, os Estados-Membros devem convidar as autoridades competentes a participar nos trabalhos do Grupo de Cooperação.

Uma avaliação europeia coordenada dos riscos

8. Os Estados-Membros devem proceder ao intercâmbio de informações entre si e com os organismos competentes da União, a fim de promover uma consciencialização comum dos riscos existentes e dos potenciais riscos de cibersegurança associados às redes 5G.

9. Os Estados-Membros devem transmitir as suas avaliações nacionais dos riscos à Comissão e à Agência Europeia para a Cibersegurança (ENISA) até 15 de julho de 2019.

10. A Agência Europeia para a Cibersegurança (ENISA) deve completar um levantamento do panorama de ameaças específicas às redes 5G. O Grupo de Cooperação e a Rede de Equipas de Resposta a Incidentes de Segurança Informática, criada ao abrigo da Diretiva (UE) 2016/1148, devem apoiar este processo.

11. Tendo em conta todos estes elementos, os Estados-Membros, com o apoio da Comissão e em conjunto com a Agência Europeia para a Cibersegurança (ENISA), devem completar, até 1 de outubro de 2019, uma revisão conjunta da exposição de toda a União aos riscos relacionados com as infraestruturas subjacentes ao ecossistema digital, em especial as redes 5G.

12. Esta revisão conjunta deve dar prioridade a uma análise dos riscos aplicável aos elementos particularmente sensíveis ou vulneráveis incluídos nos elementos principais das redes 5G, ao centro de operações e manutenção, bem como aos elementos de acesso às redes 5G utilizados em aplicações industriais.

13. Numa segunda fase, esta revisão conjunta deve ser alargada a outros elementos estratégicos da cadeia de valor digital.

Um conjunto de instrumentos comuns a nível da União para enfrentar os riscos

14. Os trabalhos no âmbito do Grupo de Cooperação devem identificar as melhores práticas do tipo previsto no ponto 4 aplicadas a nível nacional. Com base nestas melhores práticas nacionais, deve ser acordado, até 31 de dezembro de 2019, um conjunto de medidas adequadas, eficazes e proporcionadas de gestão dos riscos possíveis com vista a atenuar os riscos de cibersegurança identificados a nível nacional e da União, a fim de aconselhar a Comissão sobre a elaboração de requisitos comuns mínimos para assegurar um nível elevado de cibersegurança das redes 5G em toda a União.

15. Este conjunto de instrumentos deve incluir:

    a) Um inventário dos tipos de riscos de segurança que podem afetar a cibersegurança das redes 5G (por exemplo, risco para a cadeia de abastecimento, risco de vulnerabilidade do *software*, risco de controlo do acesso, riscos decorrentes do quadro jurídico e político a que os fornecedores de equipamentos de tecnologias da informação e das comunicações podem estar sujeitos em países terceiros) e

    b) Um conjunto de medidas de atenuação possíveis (por exemplo, certificação por terceiros para *hardware*, *software* ou serviços, ensaios formais de *hardware* e *software* ou verificações de conformidade, processos para assegurar a existência e o cumprimento de controlos de acesso, identificação de produtos, serviços ou fornecedores considerados potencialmente não seguros, etc.). Estas medidas devem incidir em todos os tipos de riscos de segurança identificados num ou mais Estados-Membros na sequência da avaliação dos riscos.

16. Uma vez desenvolvidos os sistemas europeus de certificação da cibersegurança relevantes para as redes 5G, os Estados-Membros devem adotar, em conformidade com o direito da União, regulamentação técnica nacional que preveja a certificação obrigatória de produtos, serviços ou sistemas de tecnologias da informação e das comunicações abrangidos por esses sistemas.

17. Os Estados-Membros, juntamente com a Comissão, devem identificar as condições relativas à segurança das redes públicas contra o acesso não autorizado a associar aos requisitos gerais de autorização e segurança relativos às redes com vista a solicitar compromissos às empresas que participam nos procedimentos de concessão de direitos de utilização do espetro nas faixas 5G de acordo com a Diretiva 2002/20/CE. Estes devem refletir-se, sempre que possível, nas medidas tomadas no âmbito do ponto 4, alínea c).

18. Os Estados-Membros devem cooperar com a Comissão no sentido de desenvolver requisitos de segurança específicos que possam ser aplicados no contexto dos contratos públicos relacionados com as redes 5G. Tal deve incluir requisitos obrigatórios para a implementação de sistemas de certificação da cibersegurança nos contratos públicos, na medida em que esses sistemas ainda não sejam vinculativos para todos os fornecedores e operadores.

V. **REVISÃO**

19. Os Estados-Membros devem cooperar com a Comissão a fim de, até 1 de outubro de 2020, procederem à avaliação dos efeitos da presente recomendação, com vista a determinar a via mais adequada a seguir. Esta avaliação deve ter em conta o resultado da avaliação coordenada dos riscos a nível da União e o conjunto de instrumentos da União.

Feito em Estrasburgo, em 26 de março de 2019.

Pela Comissão

Julian KING

Membro da Comissão