Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Implantação segura de redes 5G — Aplicação do conjunto de instrumentos da UE»

[COM(2020) 50 final]

(2020/C 429/37)

Relator: **Alberto MAZZOLA**

Correlator: **Dumitru FORNEA**

Consulta	Comissão Europeia, 9.3.2020
Base jurídica	Artigo 304.º do Tratado sobre o Funcionamento da União Europeia
Competência	Secção dos Transportes, Energia, Infraestruturas e Sociedade da Informação
Adoção em secção	3.9.2020
Adoção em plenária	16.9.2020
Reunião plenária n.º	554
Resultado da votação	217/0/2
(votos a favor/votos contra/abstenções)	

1. **Conclusões e recomendações**

1.1 O Comité Económico e Social Europeu (CESE) saúda a iniciativa dos Estados-Membros e da Comissão Europeia de proceder à verificação da situação no que respeita à aplicação, por parte dos Estados-Membros, das medidas recomendadas nas conclusões do conjunto de instrumentos que identifica medidas estratégicas e técnicas, bem como medidas fundamentais de segurança no âmbito da implantação do ecossistema 5G.

1.2 O CESE considera que — face à crescente complexidade e variedade de aplicações da tecnologia 5G (a Comissão estabeleceu os seguintes objetivos de conectividade para 2025: as escolas, as universidades, os centros de investigação, os hospitais, os principais prestadores de serviços públicos e as empresas que fazem uso intensivo das tecnologias digitais devem ter acesso a velocidades de carregamento/descarregamento na Internet de um *gigabit* de dados por segundo; as famílias nas zonas urbanas e rurais devem ter acesso à conectividade com uma velocidade de descarregamento de, pelo menos, 100 *megabits* por segundo; as zonas urbanas, as principais rodovias e ferrovias devem ter cobertura 5G ininterrupta) — esta verificação do ecossistema 5G, assim como das ações da competência da Comissão com vista à salvaguarda da cibersegurança das redes 5G e da diversidade da cadeia de valor 5G, da normalização técnica e da certificação, do investimento direto estrangeiro, da defesa comercial e da concorrência, das obrigações de serviço público, da contratação pública e ainda da ciberdiplomacia, deve prender-se com a segurança geopolítica, com a segurança das infraestruturas e dos dados, assim como com a proteção da saúde, nos termos do artigo 168.º, n.º 1, do TFUE.

1.3 Segundo o CESE, é importante que o ecossistema europeu 5G assegure integridade, confidencialidade, responsabilidade administrativa e operacional, segurança, fungibilidade do abastecimento, interoperabilidade dos componentes de *hardware* e *software*, normas técnicas e regulamentares comuns, continuidade de serviço, fiabilidade de fluxo e proteção dos dados, cobertura em todas as zonas, mesmo que escassamente povoadas, clareza de comunicação com o utilizador como sujeito ativo no mercado digital e ainda adesão dinâmica às orientações da Comissão Internacional para a Proteção contra as Radiações Não Ionizantes (CIPRNI) para a proteção da saúde da população, reduzindo a radiação o mais possível. A CIPRNI atualizou, em conformidade, a secção das orientações de 1998 sobre os campos eletromagnéticos de radiofrequências. No documento, apresenta essas orientações revistas, que estabelecem a proteção da exposição do ser humano a campos eletromagnéticos de 100 kHz a 300 GHz [*Health Phys*, 118(5), pp. 483-524, 2020, março de 2020]. Em 2020, a CIPRNI fez várias alterações para garantir que as novas tecnologias, como a 5G, não são suscetíveis de prejudicar a saúde humana, independentemente das nossas expectativas atuais.

1.4 O CESE exorta a Comissão a acompanhar rigorosamente os progressos na implantação e real utilização da tecnologia 5G e insta os Estados-Membros a acelerar ainda mais o processo e a zelar por uma execução responsável, tendo em conta todos os aspetos da segurança e proteção, incluindo os relacionados com o impacto da tecnologia 5G na saúde das populações e dos ecossistemas vivos, o impacto socioeconómico e na concorrência, o impacto na educação e formação e a garantia do respeito pelos direitos fundamentais.

1.5 O CESE exorta a UE a assumir a liderança mundial na próxima geração da tecnologia móvel 5G, com uma infraestrutura digital segura enquanto elemento constitutivo robusto de uma nova estratégia industrial moderna da Europa, mediante uma mudança radical na conectividade móvel, e com um enorme potencial dinâmico para aumentar a produtividade e fazer crescer a economia e os serviços destinados aos cidadãos.

1.6 Em particular, o CESE considera fundamental garantir avaliações do perfil de risco dos fornecedores e aplicar restrições adequadas aos fornecedores considerados de alto risco, incluindo as exclusões necessárias para atenuar efetivamente os riscos e para definir as responsabilidades no que respeita a ativos essenciais definidos como críticos e sensíveis na avaliação coordenada dos riscos na UE.

1.7 O CESE considera essencial que a Europa se concentre na autonomia e na autossuficiência neste domínio a médio prazo, mediante um apoio forte à investigação e a várias empresas europeias. O CESE sublinha a importância de aumentar os recursos da UE para a investigação e o desenvolvimento (I&D) no setor digital e o investimento dos operadores e fornecedores em novas funcionalidades técnicas de segurança, investimentos esses que devem poder acompanhar a capacidade do mercado de reconhecer e remunerar todas as iniciativas que visam reforçar a segurança e a resiliência dos sistemas.

1.8 Importa dar garantias de segurança a todos os Estados-Membros, nomeadamente através da manutenção de centros de investigação em várias zonas do território da UE. O CESE mantém ainda a recomendação de que haja, pelo menos, dois fornecedores por país em que pelo menos um deles seja europeu e possa garantir a segurança dos dados politicamente sensíveis e o respeito pelas restrições em matéria de saúde.

1.9 Cumpre, na opinião do CESE, dar maior ênfase aos instrumentos destinados aos utilizadores, cidadãos e organizações pertinentes da sociedade civil, que são limitados e ineficazes, para além da ênfase corretamente dada às medidas adequadas relativas às competências das entidades reguladoras nacionais e ao papel dos operadores de telecomunicações, com o objetivo de promover o empoderamento do consumidor, reforçando as suas capacidades para o tornar um sujeito proativo no mercado.

1.10 A Comissão Europeia, o Parlamento Europeu e o Conselho, assim como os governos e parlamentos dos Estados-Membros, devem disponibilizar um quadro democrático de consulta, no âmbito do qual os temas científicos ou tecnológicos, as garantias legais e as respostas das instituições competentes às questões da sociedade civil possam ser apresentados ao público.

1.11 O CESE recomenda o reforço da ciberdiplomacia europeia, para que a UE assegure condições mais equilibradas e recíprocas em matéria de trocas comerciais e investimento, especialmente no que diz respeito ao acesso das empresas ao mercado, a subsídios, contratos públicos, transferências de tecnologia, propriedade industrial e a normas sociais e ambientais.

2. **Introdução**

2.1 A segurança das redes 5G é uma questão de importância estratégica para os cidadãos e as empresas, para todo o mercado único e para a soberania tecnológica da UE. Já em 2013 a Comissão lançara a iniciativa emblemática da UE que criou uma parceria público-privada para a tecnologia 5G (PPP 5G) por forma a acelerar a investigação e a inovação neste domínio.

2.2 A tecnologia 5G, cujas receitas a nível mundial deverão atingir mais de 100 mil milhões de euros em 2025, é uma ferramenta essencial para assegurar a competitividade da Europa no mercado mundial, sendo a sua cibersegurança crucial para a autonomia estratégica da União.

2.3 As redes 5G assentam na atual quarta geração (4G) das tecnologias de rede e nas infraestruturas de fibra ótica, oferecendo novas capacidades de serviços e tornando-se na infraestrutura central e no elemento facilitador de setores alargados da economia da União, por forma a constituir a espinha dorsal de uma vasta gama de serviços essenciais ao funcionamento do mercado interno e à manutenção e gestão de funções económicas e sociais vitais, como a energia, os transportes, os serviços bancários e de saúde, assim como os sistemas agrícolas e industriais de produção, distribuição e consumo.

2.4 Dado o papel central das redes 5G na transformação digital da economia e da sociedade da UE, e dada a natureza interligada e transnacional das infraestruturas subjacentes ao ecossistema digital e a natureza transfronteiras dos riscos envolvidos, eventuais vulnerabilidades e/ou incidentes de cibersegurança significativos nas redes 5G que se verifiquem num Estado-Membro afetam a União no seu conjunto. Por esse motivo, devem ser previstas medidas que assentem num elevado nível comum de cibersegurança das redes 5G.

2.5 Em 2016, no quadro de um conjunto de iniciativas com base na Comunicação «Conectividade para um Mercado Único Digital Concorrencial — Rumo a uma Sociedade Europeia a *Gigabits*» ([1]) ([2]) e também de uma reforma do enquadramento regulamentar das comunicações eletrónicas ([3]) e das funções do Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE) ([4]), das prioridades de normalização no domínio das TIC para o mercado único digital ([5]), bem como das medidas de promoção da conectividade à Internet em comunidades locais ([6]), a Comissão adotou um plano de ação da UE para a tecnologia 5G ([7]), sobre o qual o CESE se pronunciou favoravelmente ([8]), a fim de incrementar os esforços da UE na implantação de infraestruturas e serviços 5G no mercado único digital, com um roteiro para os investimentos públicos e privados em infraestrutura 5G na UE e um objetivo de lançamento das redes comerciais 5G até 2020.

2.6 De acordo com a definição apresentada na recomendação da Comissão ([9]), entende-se por «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 ultraelevada ou que suportem um grande número de dispositivos conectados».

2.7 A recomendação indica que a Comissão apoiará a implementação de uma abordagem da União em matéria de cibersegurança das redes 5G, e trabalhará, conforme solicitado pelos Estados-Membros, no sentido de garantir a segurança da infraestrutura 5G e da cadeia de abastecimento, utilizando, sempre que necessário, todos os instrumentos à sua disposição:

— regras relativas às telecomunicações, às tecnologias multimédia e à cibersegurança;

— coordenação no domínio da normalização e certificação a nível da UE;

— regime de análise do investimento direto estrangeiro para proteger a cadeia de abastecimento da tecnologia 5G europeia;

— instrumentos de defesa comercial;

— regras de concorrência;

— contratos públicos que garantam que os aspetos relacionados com a segurança são devidamente tomados em consideração;

— programas de financiamento da UE, garantindo que os beneficiários cumprem os requisitos de segurança correspondentes.

2.8 Em julho de 2019, os Estados-Membros apresentaram os resultados das suas avaliações dos riscos nacionais ao Grupo de Cooperação previsto na Diretiva SRI ([10]) (composto por representantes de cada Estado-Membro), à Comissão e à ENISA, com informações sobre as principais atividades, ameaças e vulnerabilidades nos termos da norma ISO/IEC 27005, relativas à infraestrutura 5G e aos principais cenários de risco, descrevendo as potenciais vias através das quais os autores das ameaças podem explorar vulnerabilidades de uma atividade. Essas avaliações nacionais constituíram a base para uma avaliação subsequente coordenada e para um «conjunto de instrumentos» comuns respeitantes a possíveis medidas de atenuação do risco.

2.9 Em outubro de 2019, o Grupo de Cooperação SRI, com o apoio da Comissão e da ENISA, apresentou um relatório sobre a avaliação coordenada em toda a UE dos riscos para a cibersegurança das redes de quinta geração (5G), no qual eram identificados vários desafios importantes para a segurança relacionados com inovações tecnológicas fundamentais de *software*, aplicações e serviços, assim como com o papel dos fornecedores na implantação e utilização das redes 5G e o grau de dependência de um único fornecedor:

— maior exposição a ataques e maior número de potenciais pontos de acesso para os autores desses ataques;

— maior sensibilidade dos novos recursos de arquitetura e funcionalidades das redes 5G;

— riscos ligados à dependência dos operadores de redes móveis em relação aos fornecedores, com um aumento do número de possibilidades de ataque suscetíveis de serem exploradas pelos autores de ameaças;

([1]) Artigo 168.º, n.º 1, do TFUE «A ação da União, que será complementar das políticas nacionais…».
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) JO C 125 de 21.4.2017, p. 74.
([9]) Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, Cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).
([10]) 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).

— relevância do perfil de risco de cada fornecedor relativamente a possíveis interferências extra-UE;

— aumento dos riscos, decorrentes de uma elevada dependência dos fornecedores, de possíveis interrupções no abastecimento causadas por tensões comerciais ou outras;

— ameaças à disponibilidade e integridade das redes em matéria de segurança, confidencialidade e proteção da privacidade.

2.10 Todos esses desafios criam um novo paradigma de segurança que exige uma revisão do atual quadro político e de segurança aplicável ao setor e ao seu ecossistema e impõe aos Estados-Membros a adoção das medidas de atenuação necessárias.

2.11 Em 21 de novembro de 2019, a ENISA publicou um relatório sobre o panorama das ameaças específicas às redes 5G, em que apresentou a sua avaliação das ameaças relacionadas com a quinta geração das redes de telecomunicações móveis, e que complementa o relatório dos Estados-Membros da UE.

2.12 Em 29 de janeiro de 2020, o Grupo de Cooperação SRI publicou o documento «*Cybersecurity of 5G networks — EU toolbox of risk mitigating measures*» ([11]) [Cibersegurança das redes 5G — Conjunto de instrumentos da UE para medidas de atenuação dos riscos], que prevê um conjunto comum de medidas passíveis de atenuar os principais riscos de cibersegurança das redes 5G e fornecer orientações para a seleção das medidas que devem ser prioritárias nos planos de atenuação nacionais e da UE. No mesmo dia, a Comissão adotou uma comunicação de apoio ao conjunto de instrumentos da UE ([12]), a qual é objeto do presente parecer.

2.13 As principais partes interessadas na infraestrutura das redes 5G são:

— os cidadãos, os consumidores e os utilizadores finais de redes móveis 5G;

— os operadores de redes móveis: entidades que fornecem serviços de rede móvel aos utilizadores, gerindo a sua rede com a ajuda de terceiros;

— os fornecedores de operadores de rede móvel: entidades que fornecem serviços ou infraestruturas aos operadores de redes móveis, a fim de construir e/ou gerir as suas redes. Esta categoria inclui: produtores de equipamentos de telecomunicações; outros fornecedores de terceiros, como fornecedores de infraestruturas de computação em nuvem, integradores de sistemas, contratantes no setor da segurança e manutenção, produtores de equipamentos de transmissão;

— os produtores de dispositivos conectados e respetivos prestadores de serviços: entidades que fornecem objetos ou serviços que se conectam às redes 5G (por exemplo, telemóveis inteligentes, veículos conectados, saúde em linha) e respetivos componentes de serviços inseridos no plano de análise 5G, conforme definido na arquitetura assente nos serviços ou na computação de proximidade móvel («mobile edge computing»);

— outras partes interessadas, incluindo prestadores de serviços e conteúdos.

Todas essas partes interessadas são importantes para a segurança, quer em termos do contributo para a cibersegurança das redes 5G, quer enquanto potenciais pontos de entrada ou vetores de ataque. Por conseguinte, importa avaliar os riscos associados à sua posição no ecossistema 5G.

2.14 As principais categorias tradicionais de ameaças estão relacionadas com a obrigação de confidencialidade, integridade e disponibilidade. Mais especificamente, constatou-se que vários cenários de ameaças direcionadas às redes 5G dizem respeito ao seguinte:

— interrupção da rede 5G local ou global (disponibilidade);

— espionagem do tráfego de dados na infraestrutura de rede 5G (confidencialidade);

— modificação ou reencaminhamento do tráfego de dados na infraestrutura de rede 5G (integridade e/ou confidencialidade);

— destruição ou alteração de outras infraestruturas ou sistemas de informação digitais através das redes 5G (integridade e/ou disponibilidade).

2.15 As ameaças colocadas pelos Estados ou por perpetradores apoiados por um Estado são consideradas de extrema importância, na medida em que efetivamente representam os autores mais sérios e mais prováveis da ameaça, tendo em conta que podem ter motivações, intenções e, sobretudo, capacidade para levar a cabo ataques persistentes e sofisticados à segurança das redes 5G.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures
([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission

Embora muitas destas vulnerabilidades não sejam específicas das redes 5G, é provável que o seu número e importância aumentem com a tecnologia 5G, em razão do maior nível de complexidade da tecnologia e da maior dependência que, no futuro, a economia e a sociedade terão em relação a esta infraestrutura.

2.16 Tendo em conta, em especial, que as redes 5G assentarão, em grande medida, em *software*, as principais falhas de segurança, como as que resultam de processos insuficientes de desenvolvimento de *software* nos fornecedores de equipamentos, podem facilitar aos autores a inserção intencional de «funções-alçapão» («backdoor») nos produtos e dificultar ainda mais a sua deteção. Tal pode aumentar a possibilidade de a sua exploração ter um impacto negativo particularmente sério e generalizado. Numa altura em que ainda não se resolveram plenamente os problemas de cibersegurança da 4G, os problemas da 5G podem vir a crescer exponencialmente.

2.17 Há também que considerar as vulnerabilidades ligadas ao processo ou à configuração, nomeadamente:

— falta de pessoal especializado e experiente para proteger, monitorizar e manter redes 5G;

— deficiências no que respeita à adequação dos controlos internos de segurança, às práticas de monitorização e aos sistemas de gestão da segurança, bem como nas práticas de gestão dos riscos;

— inadequação dos procedimentos de segurança ou manutenção operacional, como a atualização do *software*/gestão das atualizações corretivas nas redes 5G;

— não conformidade com as normas 3GPP ou implementação incorreta das mesmas;

— deficiências ao nível da conceção ou da arquitetura da rede, incluindo a falta de mecanismos eficazes de emergência e continuidade, bem como uma configuração inadequada ou incorreta, por exemplo, na virtualização ou nos direitos de administração ou acesso;

— políticas inadequadas relativas ao acesso local e remoto a componentes da rede;

— requisitos de segurança insuficientes no processo de abastecimento. Esta vulnerabilidade pode assumir a forma de estratégias inadequadas para a seleção dos fornecedores ou a ausência de definição de prioridades em matéria de segurança relativamente a outros aspetos.

2.18 Os perfis de risco dos diferentes fornecedores devem ser avaliados com base em vários fatores, em particular: a possibilidade de o fornecedor estar sujeito a interferências de um país não pertencente à UE facilitada por fortes vínculos entre o fornecedor e o governo de um país terceiro específico; legislação de países terceiros, em especial quando não existe um sistema de pesos e contrapesos legislativos ou democráticos, o que pode dissuadir as filiais de uma empresa que exercem a sua atividade na UE de seguir a legislação da União, ou na ausência de acordos de segurança ou proteção de dados entre a UE e o país terceiro em questão; características da propriedade empresarial do fornecedor; capacidade de o país terceiro exercer qualquer forma de pressão, inclusive em relação ao local de produção do equipamento; qualidade geral dos produtos e práticas de cibersegurança do fornecedor, incluindo o grau de controlo sobre a sua cadeia de abastecimento e a prioridade correta atribuída às práticas de segurança.

2.19 Os Estados-Membros concordaram em assegurar a aplicação de medidas que permitam responder de forma adequada e proporcionada aos riscos já identificados e a eventuais riscos futuros. Comprometeram-se, em particular, a assegurar que estariam em posição de limitar, proibir e/ou impor requisitos e condições específicos, de acordo com uma abordagem assente no risco, no que respeita ao fornecimento, distribuição e funcionamento de equipamentos da rede 5G.

2.20 Nessa perspetiva, os Estados-Membros devem garantir:

— o reforço dos requisitos de segurança para os operadores de rede móvel, como controlos de acesso rigorosos, regras sobre a segurança do funcionamento e da monitorização, limitações à externalização de funções específicas;

— avaliações do perfil de risco dos fornecedores com base em critérios claros e objetivos; consequentemente, aplicação de restrições adequadas, no respeito dos princípios da proporcionalidade e da segurança jurídica, aos fornecedores considerados de alto risco, incluindo as exclusões necessárias para atenuar efetivamente os riscos, no que respeita a ativos essenciais definidos como críticos e sensíveis na avaliação coordenada dos riscos na UE;

— a aplicação de normas e boas práticas em matéria de segurança que assentem num consenso e que sejam reconhecidas e seguidas a nível mundial;

— a adoção, por parte de todos os operadores, de uma estratégia adequada de diversificação de fornecedores, a fim de evitar ou limitar qualquer dependência significativa de um único fornecedor ou de fornecedores com um perfil de risco semelhante;

— o controlo rigoroso, desde o acesso e gestão, ao funcionamento e monitorização seguros da rede, passando pela utilização da certificação, aplicável a componentes e/ou processos da rede 5G. Esta estratégia deve basear-se numa análise dos riscos levada a cabo pelos Estados-Membros e pelos operadores, a fim de que a opção por uma estratégia de diversificação de fornecedores não aumente o nível de risco para a rede do operador;

— um equilíbrio adequado entre os fornecedores a nível nacional, evitando a dependência de fornecedores considerados de alto risco e promovendo também uma maior interoperabilidade do equipamento;

— a manutenção de uma cadeia de abastecimento 5G diversificada e sustentável, de modo a evitar a dependência a longo prazo, fazendo pleno uso dos instrumentos de controlo do investimento direto estrangeiro, dos instrumentos de defesa comercial, das regras de concorrência e das regras de contratação pública da UE;

— o reforço das capacidades internas da UE no que respeita às tecnologias 5G e pós-5G, recorrendo a programas e financiamento adequados da UE, à coordenação entre Estados-Membros em matéria de normalização, reforçando as capacidades de «teste» e «auditoria» com vista à consecução de objetivos específicos de segurança e ao desenvolvimento de sistemas de certificação adequados na UE, nos termos da legislação sobre a segurança das TI, bem como à promoção da interoperabilidade.

2.21 Conforme salientado várias vezes pela Comissão, o mercado interno europeu é, e permanece, aberto a quem deseja entrar na Europa, desde que respeite regras claras e exigentes com base em critérios objetivos.

2.22 Em 6 de junho de 2020, o Conselho salientou a importância de se reforçar a soberania e a cooperação digitais na UE, bem como de criar sinergias através de programas da UE — como o Mecanismo Interligar a Europa e o Programa Europa Digital — com o desenvolvimento de competências digitais e da economia de dados. Salientou ainda a importância da inteligência artificial e da segurança das TI, assim como o papel ativo do setor digital na consecução dos objetivos do Pacto Ecológico.

3. **A comunicação da Comissão**

3.1 Em resposta ao conjunto de instrumentos da UE para a cibersegurança das redes 5G do Grupo de Cooperação SRI, a Comissão:

— esforça-se, conforme solicitado pelos Estados-Membros, no sentido de garantir a segurança da infraestrutura 5G e da cadeia de abastecimento, utilizando, sempre que necessário, todos os instrumentos à sua disposição;

— insta os Estados-Membros e as instituições a garantir a implementação de estratégias eficazes de atenuação dos riscos e a adotar medidas de coordenação adicionais a nível da UE com vista a uma abordagem concertada da cibersegurança da rede 5G;

— exorta os Estados-Membros a proceder à implementação das medidas recomendadas nas conclusões do conjunto de instrumentos da UE e a elaborar um relatório conjunto sobre a respetiva implementação, enquanto o Grupo de Cooperação SRI prossegue o trabalho no sentido de apoiar a implementação do conjunto de instrumentos;

— prevê — nos domínios da sua competência — ações de salvaguarda da cibersegurança das redes 5G e da diversidade da cadeia de valor 5G, da normalização técnica e da certificação, do investimento direto estrangeiro, da defesa comercial e da concorrência, da contratação pública e ainda da ciberdiplomacia, bem como dos seus próprios programas e fundos pertinentes, especialmente, para a I&D, a coesão e o desenvolvimento.

4. **Observações gerais**

4.1 O CESE está convicto de que as novas tecnologias 5G são capazes de transformar a forma como interagimos com o mundo, oferecendo oportunidades para novas aplicações, modelos de negócio, novos estilos de vida, fábricas inteligentes, maior produtividade e novos serviços de qualidade para o cidadão, abrindo potencialmente as portas a tecnologias revolucionárias, como veículos autónomos e sistemas avançados de produção e distribuição, além de permitir a interconexão de muitos milhares de dispositivos que devem entrar no nosso quotidiano como parte da Internet das coisas. No entanto, o CESE espera que a Comissão realize mais avaliações de impacto e estudos de viabilidade, assim como análises custo-benefício da tecnologia 5G, em comparação com a utilização da tecnologia 4G ou das telecomunicações de fibra ótica. O CESE reputa essencial que as tecnologias 5G sejam orientadas para uma melhor utilização circular dos recursos e para a redução da enorme pegada de carbono ligada ao consumo de energia. O CESE frisa a importância de reagir às mudanças sociais estruturais promovendo uma transição justa e harmoniosa e corrigindo o défice de competências, para criar postos de trabalho mais bem remunerados, flexíveis e altamente qualificados.

4.2 Os três riscos — pandemia descontrolada, medidas de política económica insuficientes e os «cisnes negros» geopolíticos — podem empurrar a economia mundial para uma depressão persistente e levar a perdas e a fugas nos mercados financeiros, justamente na altura em que todos os intervenientes da sociedade europeia estão cada vez mais conscientes de que um desenvolvimento económico sustentável **e a revolução digital em curso — de que as redes 5G são um dos instrumentos principais** — requerem medidas que visem simultaneamente a soberania tecnológica, o aumento da produtividade e uma utilização mais eficiente dos recursos disponíveis, com o apoio de um quadro jurídico-regulamentar e económico-financeiro adequado.

4.3 O CESE insta as instituições e os Estados-Membros da UE a completar o mercado único digital, incluindo o reforço das capacidades para integrar e utilizar os serviços 5G, a fim de defender e melhorar a competitividade das indústrias europeias. Exorta a Comissão a acompanhar rigorosamente os progressos na implantação e real utilização da tecnologia 5G e insta os Estados-Membros a acelerar ainda mais o processo, tendo em conta todos os aspetos da segurança e proteção, incluindo os relacionados com o impacto da tecnologia 5G na saúde das populações e dos ecossistemas vivos, o impacto socioeconómico, o impacto na concorrência, na educação e na formação e a garantia do respeito pelos direitos fundamentais, como o direito à propriedade ou o direito à privacidade e à segurança dos dados pessoais.

4.4 O CESE exorta a UE a assumir a liderança mundial na próxima geração da tecnologia móvel 5G, com uma infraestrutura digital segura enquanto elemento constitutivo robusto de uma nova estratégia industrial moderna da Europa, mediante uma mudança radical na conectividade móvel, e com um enorme potencial dinâmico para aumentar a produtividade e fazer crescer a economia e os serviços destinados aos cidadãos, ao seu bem-estar e à proteção do clima e do ambiente, colocando a UE na vanguarda da revolução das redes 5G.

4.5 Uma vez que a cibersegurança e a segurança nacional são dois aspetos indissociáveis, o CESE entende que qualquer decisão sobre a segurança nacional de um Estado-Membro deve ser encarada tendo em conta o contexto da UE e que as avaliações não técnicas devem ser aplicadas de forma objetiva, com base em critérios de avaliação do risco definidos a nível europeu e necessários para garantir um ambiente regulamentar previsível e harmonizado em toda a Europa, que assegure a interoperabilidade total.

4.6 O CESE considera que a qualidade da informação e os métodos de comunicação — o chamado efeito de enquadramento («framing effect»), ou posição de relevância («salience») — influenciam significativamente as opções comportamentais dos destinatários. O objetivo da promoção do empoderamento do consumidor traduz-se, portanto, na identificação de instrumentos destinados a educar e reforçar as capacidades do consumidor, tornando-o um participante ativo no mercado digital. O CESE reconhece a necessidade de disponibilizar aos cidadãos informações atualizadas e corretas sobre os benefícios e riscos da tecnologia 5G, com base no consenso da grande maioria da comunidade científica, assinalando os aspetos em que esse consenso não está garantido.

4.7 O CESE está convicto de que o acesso ao mercado digital europeu deve continuar a ser livre para qualquer empresa sem discriminação, mas sem prejuízo do respeito por um quadro europeu de regras, normas e critérios de avaliação e de segurança rigorosos e claros que coloquem no centro da estratégia europeia a recuperação e revitalização da sua soberania tecnológica.

4.8 Embora entre os cinco principais fornecedores de infraestruturas se incluam dois fornecedores europeus, dois chineses e um coreano ([13]), nenhuma grande empresa europeia está entre as primeiras a produzir dispositivos e conjuntos de chipes 5G. O CESE está convencido de que se deve assegurar a presença de vários fornecedores, sendo pelo menos um de propriedade europeia, assim como um quadro de interoperabilidade e fungibilidade total dos componentes de *hardware* e *software*, a fim de garantir também a plena soberania tecnológica europeia no âmbito de uma forte cooperação internacional e de total reciprocidade na abertura, acesso e funcionamento dos mercados. Uma tal diversificação é viável contanto que a interoperabilidade dos serviços seja possível e que a diversidade não aumente os riscos para a cibersegurança.

4.9 O CESE considera essencial que a Europa se concentre na autonomia e na autossuficiência neste domínio a médio prazo, mediante um apoio forte à investigação e a várias empresas europeias. Acolhe favoravelmente o conjunto de medidas decidido pelos Estados-Membros para fazer face aos riscos de segurança e proteção associados à introdução da tecnologia 5G, já identificados na avaliação europeia. Considera, no entanto, que devem ser aplicados limites de exposição a campos eletromagnéticos rigorosos e seguros, tal como recomendado a nível da UE, com base em informações atualizadas da Comissão Internacional para a Proteção contra as Radiações Não Ionizantes (CIPRNI), reconhecida pela Organização Mundial da Saúde (OMS), e que esses limites devem aplicar-se a todas as faixas de frequência previstas para a tecnologia 5G ([14]). Os limites da CIPRNI assentam no princípio da precaução, uma vez que são 50 vezes inferiores aos efeitos sobre a saúde pública, com base nos dados científicos disponíveis.

([13]) Atualmente, os cinco fornecedores mundiais são: Ericsson, Nokia, Huawei, ZTE e Samsung.
([14]) PE — E-003040/2019, resposta dada por Stella Kyriakides em nome da Comissão Europeia (17.1.2020).

4.10 No entanto, o CESE observa que os limites da CIPRNI não são reconhecidos por toda a comunidade, havendo alguns cientistas que preconizam limites de exposição da população muito mais rigorosos, de acordo com o princípio de assegurar um risco tão baixo quanto razoavelmente possível. Algumas das soluções que podem ser propostas para complementar as infraestruturas de comunicações 5G passam pelo recurso a conexões de dados fixas utilizadas por tecnologias não rádio (cabos Ethernet, fibra ótica, etc.) em situações em que a utilização é fixa (por exemplo, caixas automáticas, pontos de venda bancários, robôs industriais, robôs médicos controlados à distância, etc.) e em que os utilizadores transmitem vastas quantidades de dados (prestadores de serviços digitais, empresas/sociedades, etc.); na Internet das coisas utilizada em locais fixos, não móveis (residência inteligente, cidade inteligente, sensores presentes em equipamento de empresas de serviços públicos, etc.).

4.11 A Comissão Europeia, o Parlamento Europeu e o Conselho, assim como os governos e parlamentos dos Estados-Membros, devem disponibilizar um quadro democrático de consulta, no âmbito do qual os temas científicos ou tecnológicos, as garantias legais e as respostas das instituições competentes às questões da sociedade civil possam ser apresentados ao público.

4.12 Cumpre, na opinião do CESE, dar maior ênfase aos instrumentos destinados aos utilizadores, cidadãos e organizações pertinentes da sociedade civil, que são limitados e ineficazes, para além da ênfase corretamente dada às medidas adequadas relativas às competências das entidades reguladoras nacionais e ao papel dos operadores de telecomunicações.

4.13 O CESE reconheceu ([15]) a prevalência da hipersensibilidade eletromagnética e manifestou a sua preocupação com a questão, considerando encorajador constatar que estão em curso trabalhos de investigação aprofundada para compreender o problema e as suas causas. Insta a Comissão a prosseguir e atualizar o trabalho nesse domínio.

4.14 No entender do CESE, a credibilidade dos prestadores de serviços de telecomunicações e de aplicações 5G é essencial, uma vez que a gestão da informação na Internet constitui a base dos serviços de dados agregados recolhidos e processados pelos utilizadores por meio de mecanismos tecnológicos, legais e fiscais, colocando em inter-relação direta objetos, máquinas e algoritmos.

4.15 O CESE recomendou ([16]) que se transitasse do conceito de propriedade de dados para a definição de «direitos em relação aos dados» para as pessoas singulares e as pessoas coletivas. Os consumidores devem poder controlar os dados produzidos pelos dispositivos conectados a fim de garantir a privacidade dos consumidores e a acessibilidade, a interoperabilidade e a transferência de dados, assegurando ao mesmo tempo uma proteção e uma confidencialidade dos dados adequadas, a concorrência leal e uma escolha mais ampla por parte dos consumidores.

4.16 O Regulamento Geral sobre a Proteção de Dados (RGPD) deve ser enriquecido com disposições de execução claras que permitam obter uma aplicação uniforme e um elevado nível de proteção dos dados e dos consumidores, à luz da interconectividade de máquinas e objetos, e rever as normas sobre a responsabilidade civil e os seguros de produtos, com vista à sua adaptação a uma situação em que as decisões serão cada vez mais tomadas pelo *software* num quadro de total segurança.

4.17 O CESE considera essencial que os Estados-Membros sigam as recomendações estratégicas e técnicas constantes do conjunto de instrumentos da UE, evitando o desenvolvimento de abordagens nacionais específicas, como, por exemplo, testes e certificações adicionais, que causariam uma fragmentação do mercado, atrasos na implantação das tecnologias e inconsistências entre os mercados, com o risco de minar a confiança nos sistemas de teste e certificação.

4.18 O CESE considera essencial o recurso a normas mundiais, com um apoio acrescido por parte da Europa, e a boas práticas partilhadas e reconhecidas, a fim de permitir uma gestão eficiente das ameaças, gerar economias de escala, evitar a fragmentação e garantir a interoperabilidade dos sistemas europeus. As conversações sobre normas técnicas trarão a clarificação necessária para que as empresas voltem a competir e a liderar essas atividades fundamentais que possibilitam implantar tecnologias avançadas, como as redes 5G e a inteligência artificial, em todos os mercados.

4.19 Em particular, o CESE considera fundamental avaliar o perfil de risco dos fornecedores e impor restrições adequadas aos fornecedores considerados de alto risco, incluindo as exclusões necessárias para atenuar efetivamente os riscos no que respeita a ativos essenciais definidos como críticos e sensíveis na avaliação coordenada dos riscos na UE.

4.20 O CESE sublinha a importância de aumentar os investimentos dos operadores e fornecedores em novas funcionalidades técnicas de segurança, investimentos esses que devem poder acompanhar a capacidade do mercado de reconhecer e remunerar todas as iniciativas que visam reforçar a segurança e a resiliência dos sistemas. Uma maior visibilidade dos investimentos em segurança poderá introduzir novos elementos de recompensa do mercado.

([15]) JO C 242 de 2.7.2015, p. 31.
([16]) JO C 353 de 18.10.2019, p. 79.

4.21 O CESE apoia firmemente intervenções comuns de apoio ao desenvolvimento industrial e à implantação das tecnologias 5G: avaliação de possíveis falhas ou lacunas no mercado ao longo da cadeia de valor 5G, de modo a justificar intervenções específicas no quadro do próximo orçamento de longo prazo ou de um possível projeto de interesse europeu comum em matéria de cibersegurança 5G (segurança e proteção).

4.22 O CESE salienta que, embora a infraestrutura digital se tenha mostrado resistente e robusta durante a crise da COVID-19, são necessários mais investimentos em infraestruturas 5G a fim de superar a fratura digital que ainda existe e que pode limitar o acesso dos cidadãos à saúde em linha, à aprendizagem eletrónica e ao trabalho à distância.

4.23 No plano da ciberdiplomacia, o CESE considera essencial que a UE assegure condições mais equilibradas e recíprocas em matéria de trocas comerciais e investimento, especialmente no que diz respeito ao acesso das empresas ao mercado, subsídios, contratos públicos, transferências de tecnologia, propriedade industrial e normas sociais e ambientais, sobretudo na presença de «rivais sistémicos que promovem modelos alternativos de governação», incentivando simultaneamente a plena concorrência e a inovação técnica no mercado.

4.24 O CESE apoia firmemente a necessidade de manter uma cadeia de abastecimento 5G diversificada e sustentável, a fim de evitar dependências a longo prazo, prevendo a presença de vários fornecedores num quadro de fungibilidade e interoperabilidade, e de reforçar ainda mais, no âmbito do Quadro Financeiro Plurianual 2021-2027, os programas e as iniciativas com vista a fortalecer as capacidades e a soberania tecnológica europeia 5G e pós-5G.

4.25 No contexto do plano de recuperação para a Europa, adotado em 27 de maio de 2020, o índice de digitalidade da economia e da sociedade 2020 (IDES) servirá de base para a análise específica por país, apoiando as recomendações do Semestre Europeu no domínio digital. Ajudar-se-á, assim, os Estados-Membros a orientar e estabelecer as prioridades no que respeita às respetivas necessidades de reforma e investimento, facilitando, desse modo, o acesso ao Mecanismo de Recuperação e Resiliência no valor de 560 mil milhões de euros. Este mecanismo proporcionará aos Estados-Membros os fundos para tornar as respetivas economias mais resilientes e garantir que os investimentos e as reformas apoiam as transições ecológica e digital. Uma vez que a pandemia teve um impacto significativo em cada uma das cinco dimensões do IDES, as conclusões respeitantes a 2020 devem ser lidas tendo em mente as numerosas medidas adotadas pela Comissão e pelos Estados-Membros para gerir a crise e apoiar a recuperação.

Bruxelas, 16 de setembro de 2020.

O Presidente
do Comité Económico e Social Europeu
Luca JAHIER