Parecer do Comité Económico e Social Europeu — Comunicação conjunta ao Parlamento Europeu e ao Conselho — Política de ciberdefesa da UE

(parecer de iniciativa)

(2023/C 293/04)

Relator: **Anastasis YIAPANIS**

Correlator: **Alberto MAZZOLA**

Decisão da Plenária	20.9.2022
Base jurídica	Artigo 52.º, n.º 2, do Regimento
	Parecer de iniciativa
Competência	Comissão Consultiva das Mutações Industriais (CCMI)
Adoção em secção	27.3.2023
Adoção em plenária	14.6.2023
Reunião plenária n.º	579
Resultado da votação	
(votos a favor/votos contra/abstenções)	208/1/2

1. **Conclusões e recomendações**

1.1. O Comité Económico e Social Europeu (CESE) apoia a política de ciberdefesa da UE proposta, mas esperava que a sociedade civil organizada tivesse um papel mais proeminente na elaboração das propostas. Nesta fase, o Comité considera difícil avaliar se as futuras iniciativas delineadas na comunicação conjunta serão aplicadas e se alcançarão os resultados pretendidos. Solicita às instituições da UE e aos Estados-Membros que deem prioridade e façam avançar rapidamente as iniciativas anunciadas.

1.2. O CESE salienta a necessidade de medidas adicionais para reforçar a capacidade da UE de detetar ciberameaças e apela para que o financiamento da investigação e desenvolvimento (I&D) seja canalizado para o desenvolvimento de capacidades de ponta da UE. A cooperação entre os setores público e privado é essencial e não deve ser unidirecional. O CESE considera necessária a coordenação da UE para combater a fragmentação e assegurar a cooperação e o investimento conjunto entre os Estados-Membros.

1.3. O CESE apoia a criação do centro de coordenação da ciberdefesa da UE e recomenda que os Estados-Membros se comprometam a dar uma resposta rápida 24 horas por dia, sete dias por semana, e avaliem a prontidão frente a ciberataques e o desempenho dos mecanismos da UE de resposta a cibercrises, com um foco nas capacidades militares e nos setores críticos identificados pela Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho (Diretiva SRI 2) ([1]). O Comité apoia o alargamento do mandato do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, por forma a apoiar o trabalho do centro de coordenação da ciberdefesa da UE.

1.4. Para reforçar a autonomia estratégica e a soberania da União no domínio da cibersegurança, o CESE considera que importa desenvolver, ou adotar do setor privado, uma plataforma que permita a realização de testes e a partilha de informações de forma dinâmica e em tempo real, a fim de identificar as atuais lacunas nas capacidades existentes. Esta pode ser usada também para partilhar boas práticas, comunicar ciberincidentes e criar uma lista da UE de todos os cibercriminosos.

([1]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333, 27.12.2022, p. 80).

1.5. O CESE salienta a necessidade de uma melhor preparação contra ciberataques, como os russos na Ucrânia, especialmente os que visem infraestruturas críticas. A cooperação entre os ecossistemas civil e militar é crucial para uma gestão eficiente das crises, para a interoperabilidade e para evitar a duplicação de esforços e de investimentos, nomeadamente através de ciberataques simulados para efeitos de teste.

1.6. O CESE considera que os investimentos na ciberdefesa devem dar prioridade à proteção dos cidadãos e das infraestruturas críticas da UE, nomeadamente através da utilização de fornecedores de *hardware* e *software* seguros. Insiste em que as prioridades e os investimentos sejam atualizados em momento oportuno e sejam objeto de acordo entre a UE e os Estados-Membros, com a participação das partes interessadas pertinentes do setor privado.

1.7. A UE deve manter e desenvolver as capacidades necessárias para garantir a sua economia digital, sociedade, democracia e tecnologias críticas, bem como para prestar serviços de cibersegurança essenciais. Para assegurar a autonomia estratégica da UE, é crucial reduzir as dependências em relação a países terceiros. O CESE considera essencial que a UE adote uma abordagem de médio prazo destinada a assegurar a autonomia no domínio das tecnologias fulcrais, e preconiza firmemente a criação de instalações de investigação e de produção por parte de empresas sediadas na UE, com uma política industrial europeia adequada, centrada num ecossistema cibernético autónomo.

1.8. As pequenas e médias empresas (PME) devem receber apoio específico e ter acesso a programas de financiamento que aumentem a sua resiliência a ciberataques, bem como acesso a oportunidades de assistência, formação e educação sobre os ciber-riscos e as formas de se protegerem dos mesmos. A UE deve proporcionar um mecanismo de incentivo que fomente uma familiarização gradual das PME e o desenvolvimento de PME inovadoras.

1.9. O CESE apoia o plano de criação de uma academia de cibercompetências e solicita à Comissão Europeia que coordene e financie ações de formação em grande escala e programas de formação e ensino profissionais, que envolvam todos os Estados-Membros e visem a criação de mão de obra qualificada para todas as agências e organizações relacionadas com a ciberdefesa, bem como para as redes civis privadas.

1.10. O Comité considera crucial sensibilizar os cidadãos para a cibersegurança, a fim de reduzir a exposição a ciberataques, e apela para a criação de programas de ensino e de formação ao longo da vida sobre a cibersegurança, que se centrem na melhoria das cibercompetências e dos ciberconhecimentos. O CESE apoia a integração da cibersegurança em todas as futuras políticas públicas da UE e a realização de ações de informação do público em geral sobre ciberameaças.

1.11. O CESE considera que uma forte cooperação com os aliados da OTAN em domínios militares deve incidir na plena coordenação e reciprocidade, em projetos conjuntos de investigação, desenvolvimento e inovação, na partilha de boas práticas, em programas de formação de grande dimensão e em simulações de ciberataques, com o principal objetivo de melhorar a capacidade de resposta comum.

1.12. O Comité insta o Alto Representante a analisar os atuais ciberdiálogos bilaterais e a encetar debates adicionais com outros países e organizações internacionais pertinentes, a fim de estabelecer um quadro mundial para a adesão ao direito internacional no ciberespaço, com uma forte ênfase na reciprocidade. O Comité considera que a UE está bem preparada para liderar os debates internacionais sobre o futuro da cibersegurança, em particular no âmbito das Nações Unidas, uma vez que tem uma base sólida no que toca às liberdades democráticas fundamentais.

1.13. A UE deve assumir uma posição firme contra qualquer tipo de sistema de classificação social aplicado aos cidadãos. O CESE esclarece que não pode haver verdadeira democracia sem uma proteção dos dados pessoais eficaz e considera essencial uma gestão de dados responsável e eficiente para transformar a hiperconectividade numa vantagem concorrencial.

2. **Introdução e observações gerais**

2.1. A expansão digital das sociedades acarreta um grande número de ameaças à cibersegurança, geradas pelas melhorias tecnológicas. Os ciberataques aumentaram significativamente em número e sofisticação nos últimos anos, comprometendo a segurança de entidades públicas e privadas. Quer se trate de *software* de sequestro, *software* malicioso, ataques por correio eletrónico, violações de dados, desinformação, ataques distribuídos de negação de serviço ou outras formas de ataques, todos eles constituem uma ameaça firme e constante para a segurança da UE no seu conjunto.

2.2. O CESE congratula-se com a Comunicação conjunta — Política de ciberdefesa da UE ([2]) e considera que agora é o momento de agir, com urgência e de forma coordenada a nível da UE, envolvendo os ecossistemas civil e militar do ciberespaço e assegurando o quadro de investimento adequado para as capacidades de ciberdefesa. No entanto, o Comité assinala que a comunicação é apenas uma declaração da determinação de agir, bem como uma lista de futuras iniciativas da UE que deverão produzir resultados, e considera impossível avaliar se esses compromissos futuros serão efetivamente concretizados, uma vez que as futuras negociações entre os colegisladores influenciarão, naturalmente, o resultado final do plano de ação da UE para a cibersegurança.

2.3. O ataque russo à rede de satélites KA-SAT, que perturbou a comunicação entre as forças militares ucranianas, e o recente escândalo em que Éric Léandri foi contratado por empresas do setor da defesa para realizar ações de ciberespionagem em seu nome colocam a cibersegurança no topo da lista de ameaças à segurança na UE. Embora o Regulamento Geral sobre a Proteção de Dados seja um ato legislativo sólido da UE e esteja em vigor há vários anos, é evidente que a quantidade crescente de dados disponíveis está vulnerável e que o risco de terceiros transporem os limites da legalidade aumenta todos os dias.

2.4. Dada a natureza transnacional dos ciberataques, é necessária coordenação da UE para reduzir a atual fragmentação e assegurar que os Estados-Membros estão preparados para cooperar e investir em conjunto. Este aspeto é particularmente importante em casos futuros em que um Estado-Membro possa ser visado, para assegurar que todos os outros têm a oportunidade de prestar apoio imediato.

3. **Agir em conjunto para uma ciberdefesa mais forte**

3.1. O Comité toma nota das iniciativas ambiciosas anunciadas para criar um centro de coordenação da ciberdefesa da UE, desenvolver o projeto CyDEf-X, criar equipas de resposta rápida a ciberataques, desenvolver uma iniciativa da UE em matéria de cibersolidariedade e explorar o desenvolvimento de sistemas de certificação da cibersegurança para produtos, serviços e processos de tecnologias da informação e comunicação. O CESE recomenda que todos os Estados-Membros se comprometam a estar preparados para dar uma resposta rápida 24 horas por dia, sete dias por semana, cabendo ao centro de coordenação da UE participar na avaliação e elaboração de relatórios periódicos sobre o estado de prontidão frente a ciberataques dos Estados-Membros e sobre a eficácia do mecanismo europeu de resposta a cibercrises, incidindo tanto nas capacidades militares como nos setores críticos definidos na Diretiva SRI 2. Cada Estado-Membro deve dispor de especialistas especificamente formados para intervir em caso de ciberincidentes e deve testar regularmente a sua capacidade de intervenção noutros Estados-Membros.

3.2. Embora a comunicação apresente uma longa lista de melhorias a alcançar passo a passo, o CESE esperava ver um roteiro explícito para a aplicação dessas iniciativas, com uma governação clara e prazos claros para a apresentação e adoção de soluções. Além disso, o Comité esperava que fosse atribuído à sociedade civil organizada um papel mais proeminente na elaboração destas propostas.

3.3. O CESE considera que os Estados-Membros devem reforçar a sua capacidade interna para combater as ciberameaças, participando simultaneamente em projetos de cooperação e partilhando informações e boas práticas com os seus homólogos de outros Estados-Membros. É necessário um investimento rápido nas capacidades de ciberdefesa e na implantação célere da tecnologia ([3]) em todos os Estados-Membros, assim como na preparação comum para detetar e defender de ciberataques e para recuperar dos mesmos. A fim de apoiar a autonomia da União no domínio da cibersegurança, o Comité considera que deve ser desenvolvida, ou adotada do setor privado, uma plataforma que permita a realização de testes e partilha de informações de forma dinâmica e em tempo real, focada em identificar as capacidades atualmente em falta.

3.4. O CESE concorda que, nesta fase, as operações militares no ciberespaço devem continuar a ser estritamente da competência dos Estados-Membros. O Comité congratula-se com a cooperação anunciada entre as equipas militares de resposta a emergências informáticas (milCERT) da UE, as equipas de resposta a incidentes de segurança informática (CSIRT) e a equipa de resposta a emergências informáticas para as instituições e agências da UE (CERT-UE).

3.5. A Diretiva SRI 2, recentemente adotada, e a Diretiva relativa à resiliência das entidades críticas (REC) ([4]) já estabeleceram obrigações nacionais e setoriais específicas para o quadro da UE em matéria de ciberdefesa. São necessárias mais ações para melhorar a capacidade coletiva da UE de detetar ciberameaças, e o CESE apela para investimento em I&D que seja canalizado para o desenvolvimento de capacidades de ponta da UE.

([2]) Comunicação da Comissão — Política de ciberdefesa da UE.

([3]) Como a iniciativa DIANA — *Defence Innovation Accelerator for the North Atlantic* [Acelerador da inovação no domínio da defesa do Atlântico Norte] da OTAN.

([4]) Diretiva REC.

4. **Proteger o ecossistema de defesa da UE**

4.1. O CESE considera que as complexidades inerentes e os desafios tecnológicos, que evoluem rapidamente, transformaram o ecossistema da defesa e que a cibersegurança se tornou um tema comum tanto para os setores militar e civil como para os cidadãos da UE. A cooperação entre os ecossistemas civil e militar é agora mais importante do que nunca e deverá gerar benefícios, como uma gestão de crises mais eficaz, progressos contínuos e interoperabilidade, evitando a duplicação ou a multiplicação dos mesmos esforços e investimentos. Os Estados-Membros devem estar prontos para realizar, a nível nacional, testes de resistência das infraestruturas críticas, a fim de avaliar e aumentar a resiliência a futuros ciberataques.

4.2. O CESE considera que os investimentos na ciberdefesa devem, a título prioritário, visar a proteção dos cidadãos e das infraestruturas críticas da UE. Dado o ritmo acelerado da transformação digital e a rápida evolução do panorama das ameaças, o Comité insta veementemente a UE e os Estados-Membros a chegarem a acordo sobre atualizações atempadas das prioridades e do investimento, consultando devidamente as partes interessadas do setor privado. Muitas vezes, os dispositivos da Internet das coisas não estão tão bem protegidos como os dispositivos tradicionais, e o CESE apela para que se garanta um nível de segurança mínimo através de plataformas de gestão da identidade e do acesso. Além disso, uma vez que a certificação é um método fundamental para proporcionar um maior nível de segurança, o Comité solicita que a nova abordagem de certificação da UE dê mais ênfase à segurança no âmbito da Internet das coisas.

4.3. A UE deve reforçar a sua resiliência frente a ciberataques e proporcionar ciberdissuasões eficazes. Há que proteger as infraestruturas críticas contra todo o tipo de ciberataques, incluindo pelos sistemas de defesa da UE. O Comité considera ser do interesse estratégico da UE assegurar que a União mantém e desenvolve as capacidades essenciais para proteger a sua economia digital, a sua sociedade e a sua democracia e para alcançar a plena soberania digital, pois é essa a única forma de proteger as tecnologias críticas e de prestar serviços de cibersegurança fulcrais eficazes. Diminuir a dependência em relação a países terceiros é também vital para a autonomia estratégica da UE. O CESE considera que as agências setoriais da UE [Agência da União Europeia para a Cibersegurança (ENISA), Agência da União Europeia para a Segurança da Aviação (EASA), Agência Ferroviária da União Europeia (ERA), Agência Europeia de Medicamentos (EMA), Autoridade Bancária Europeia (EBA), Agência Espacial Europeia (ESA), Agência de Execução Europeia da Saúde e do Digital (HADEA), etc.] devem participar no processo e fornecer orientações para o desenvolvimento de sistemas de cibersegurança.

4.4. A pandemia de COVID-19 acelerou a transição digital e transformou o trabalho tradicional em trabalho híbrido e/ou remoto, criando novas relações de trabalho e novas expectativas, bem como uma nova classe de nómadas digitais, cujo número está a aumentar. O CESE assinala as rápidas mudanças no mercado de trabalho, que geraram a adoção de uma «arquitetura de confiança zero» pelas empresas, através de soluções de gestão da identidade e do acesso e de gestão do acesso privilegiado. O Comité considera que este tipo de gestão dos recursos das empresas proporciona novas soluções relacionadas com as ciberameaças. Considera também que o setor privado deve ser apoiado para reforçar o nível de segurança das suas soluções digitais inovadoras.

4.5. O CESE está bastante desiludido com a afirmação da Comissão de que «[p]oderá ser estabelecido um plano de implementação em cooperação com os Estados-Membros» e considera um tal plano de execução imprescindível, entendendo que deve ser elaborado em conjunto com os Estados-Membros e aplicado o mais rapidamente possível. O Comité está preocupado com a abordagem pouco interventiva da Comissão e insta as instituições da UE e os Estados-Membros a facilitarem avanços rápidos nas iniciativas anunciadas.

5. **Investir em capacidades de ciberdefesa**

5.1. À medida que o desenvolvimento da tecnologia avança rapidamente, o ciberespaço tornou-se o mais recente domínio operacional, a juntar-se à terra, ao mar, ao ar e ao espaço. Gerou também grandes oportunidades de criminalidade para intervenientes mal-intencionados no espaço cibernético, que vão desde piratas informáticos independentes a criminosos profissionais e até intervenientes estatais.

5.2. O investimento em I&D é vital e o CESE congratula-se com os fundos específicos existentes no âmbito do Programa Europa Digital, do Fundo Europeu de Defesa, do Horizonte Europa e dos planos nacionais de recuperação e resiliência. No entanto, o Comité gostaria que existissem mais projetos transnacionais centrados na cooperação e na interoperabilidade entre sistemas de ciberdefesa em todos os Estados-Membros, bem como mais sinergias entre instrumentos de financiamento, em especial para acompanhar as PME inovadoras.

5.3. Tal como anunciado na Estratégia de Cibersegurança da UE, em 2020, o Comité observa que o prazo para a criação da ciberunidade conjunta termina este ano, pelo que aguarda notícias sobre a finalização do processo e a preparação da UE para responder a ciberincidentes em grande escala. O CESE espera que esta ciberunidade melhore o conhecimento da situação na UE e a capacidade global de resposta e recuperação.

5.4. O CESE apoia o alargamento do mandato do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, por forma a apoiar as atividades do centro de coordenação da ciberdefesa da UE. Além disso, esta rede poderia apoiar a soberania digital europeia através do desenvolvimento de uma base industrial europeia competitiva para capacidades tecnológicas fulcrais, baseada, em parte, no trabalho levado a cabo por parcerias público-privadas (PPP) contratuais. As PPP demonstraram ser a abordagem mais eficaz para melhorar a cibersegurança de todo o ecossistema digital, mas não podem ser unidirecionais: as instituições públicas têm também de partilhar as suas informações com o setor privado.

5.5. O CESE observa que, para fazer frente a futuras tentativas de pirataria informática a partir de computadores quânticos, a UE deve investir imediatamente em tecnologias de ponta, como a criptografia pós-quântica. O CESE considera essencial que a Europa se concentre na autonomia a médio prazo, e preconiza firmemente a criação de instalações de investigação e de produção por parte de empresas sediadas na UE. O CESE considera importante aumentar os recursos da UE disponíveis para atividades de investigação e inovação digital e apoiar o investimento dos operadores e fornecedores em novas funcionalidades técnicas de segurança, inclusivamente no domínio das tendências emergentes como a realidade aumentada e o metaverso. Especificamente, é essencial criar uma infraestrutura europeia de computação em nuvem distribuída, baseada nas regras europeias relativas a temas como o armazenamento e o tratamento de dados ([5]).

5.6. As PME devem merecer uma atenção especial e ter acesso a programas de financiamento que aumentem a sua preparação para ciberataques, bem como acesso a programas de assistência, formação e educação que as ajudem a compreender os riscos cibernéticos e as formas de se protegerem contra os mesmos. A UE deve proporcionar um mecanismo de incentivo que promova a familiarização progressiva das PME.

5.7. A Comissão estima em meio milhão de pessoas a atual escassez de competências no domínio da cibersegurança, e o CESE aprecia a proposta de criação de uma academia de cibercompetências. É evidente que os esforços a nível dos Estados-Membros não são suficientes para reduzir o défice de competências, pelo que o Comité sugere que, juntamente com o lançamento da academia, a Comissão aproveite a dinâmica proporcionada pelo Ano Europeu das Competências e coordene e financie ações de formação em grande escala e programas de ensino e formação profissionais a nível da UE, que envolvam todos os Estados-Membros e se concentrem na formação de mão de obra qualificada para todas as agências e organismos relacionados com a ciberdefesa, bem como para as redes civis privadas. Deve ser dada especial atenção à formação da mão de obra, em especial nos domínios da ciência, tecnologia, engenharia e matemática (CTEM).

5.8. Além disso, o CESE considera fundamental sensibilizar os cidadãos para a cibersegurança, a fim de reduzir a exposição a ciberataques, especialmente no que diz respeito aos cibercrimes básicos que visam a população em geral. O Comité apela à criação de programas de ensino e de formação ao longo da vida sobre a cibersegurança, que se centrem na melhoria das cibercompetências e tornem a cibersegurança mais familiar e atrativa para os cidadãos, em especial a geração mais jovem. O CESE é favorável à integração dos aspetos relacionados com a cibersegurança em todas as políticas públicas futuras da UE e à realização de ações de informação do público em geral sobre ciberameaças, nomeadamente através de programas de formação gratuitos abertos a todos os cidadãos, de aplicações informativas gratuitas para telemóveis ou de anúncios televisivos em horário nobre. Paralelamente a estas ações, importa promover um progresso cultural generalizado, a todos os níveis da sociedade, rumo a uma abordagem orientada para a cibersegurança.

5.9. O CESE considera fundamental avaliar o perfil de risco dos fornecedores e impor restrições adequadas aos fornecedores considerados de alto risco, o que inclui as proibições necessárias de aplicações e ativos essenciais considerados críticos e sensíveis na avaliação dos riscos coordenada na UE e a certificação de fornecedores de *hardware* e *software* seguros.

6. **Parcerias para dar resposta aos desafios comuns**

6.1. O nível de preparação para futuros ciberataques varia muito de um Estado-Membro para outro. O CESE considera que o primeiro passo imediato é criar uma plataforma de comunicação de boas práticas dentro da UE, na qual os Estados-Membros mais avançados no domínio cibernético possam partilhar os seus conhecimentos com os outros países e facilitar a sua aquisição imediata, o que ajudaria a melhorar a confiança mútua entre entidades nacionais. Em segundo lugar, o Comité considera necessário reforçar a cooperação entre os intervenientes estatais e não estatais em toda a UE, a fim de melhorar a cibersegurança dos produtos e serviços no mercado interno. O CESE propõe igualmente a criação de uma plataforma comum da UE para a comunicação de ciberincidentes, incluindo uma lista negra da UE de todos os responsáveis por atividades de cibercriminalidade.

([5]) Como a Gaia-X, iniciativa franco-alemã.

6.2. O CESE considera que uma forte cooperação com os nossos aliados da OTAN no domínio militar deve centrar-se não só no reforço das capacidades e na deteção precoce, mas também em projetos conjuntos de investigação, desenvolvimento e inovação, na partilha de boas práticas e no intercâmbio entre peritos, em programas de formação de grande dimensão e em simulações de ciberataques. O principal objetivo deve ser o de alargar a capacidade de resposta comum e criar sinergias para combater futuras ameaças híbridas, na sequência da Declaração Conjunta de Varsóvia, de 2016, e da Declaração Conjunta de Bruxelas, de 2018. A cooperação entre a UE e a OTAN ainda tem uma série de vias a explorar, e a realização de progressos imediatos pode fazer a verdadeira diferença no que toca a garantir a segurança dos nossos cidadãos e sociedades.

6.3. O Comité considera que os debates a nível mundial e com os nossos parceiros internacionais devem abrir caminho à promoção de um ciberespaço mundial e aberto que proteja os direitos humanos, as liberdades fundamentais e o Estado de direito e se centre na elaboração de normas internacionais vinculativas em setores com rápido desenvolvimento digital. O CESE insta o Alto Representante a analisar os ciberdiálogos bilaterais atualmente existentes e a encetar mais negociações com outros países e organizações internacionais pertinentes, a fim de promover um quadro mundial para a aplicação do direito internacional no ciberespaço, com base numa rigorosa condição de reciprocidade.

6.4. Por fim, o Comité considera que a UE é a mais bem posicionada para liderar os debates internacionais sobre o futuro da cibersegurança, em particular no âmbito dos debates nas Nações Unidas, devido à base sólida de que dispõe no que toca às liberdades democráticas fundamentais. A UE deve também empenhar-se no combate aos regimes totalitários que monitorizam os dados dos cidadãos e violam os seus direitos e liberdades, e deve posicionar-se vigorosamente contra qualquer tipo de sistema de classificação social aplicado aos cidadãos. O CESE afirma claramente que não pode haver verdadeira democracia sem uma proteção dos dados pessoais eficaz e considera que uma gestão de dados responsável e eficiente é essencial para transformar a hiperconectividade numa vantagem.

Bruxelas, 14 de junho de 2023.

O Presidente
do Comité Económico e Social Europeu
Oliver RÖPKE