Parecer do Comité Económico e Social Europeu sobre «Confiança, privacidade e segurança para os consumidores e as empresas na Internet das coisas (IdC)»

[parecer de iniciativa]

(2018/C 440/02)

Relator: **Carlos TRIAS PINTÓ**

Correlator: **Dimitris DIMITRIADIS**

Decisão da plenária	15.2.2018
Base jurídica	Artigo 29.º, n.º 2, do Regimento Parecer de iniciativa
Competência	Secção Especializada do Mercado Único, Produção e Consumo
Adoção em secção	4.9.2018
Adoção em plenária	19.9.2018
Reunião plenária n.º	537
Resultado da votação (votos a favor/votos contra/abstenções)	182/3/2

1. Conclusões e recomendações

1.1. A Internet das Coisas (a seguir designada «IdC»), ao interconectar pessoas e objetos, oferece aos cidadãos e às empresas um imenso leque de oportunidades que devem ser acompanhadas de um conjunto de garantias e controlos destinados a assegurar uma implantação satisfatória.

1.2. Tendo em conta que um dos pilares da IdC é a tomada de decisões automática e sem intervenção humana, é necessário garantir que tais decisões não sejam contrárias aos direitos dos consumidores, não acarretem qualquer risco de carácter ético nem sejam contrárias aos princípios e direitos humanos fundamentais.

1.3. O CESE insta as instituições europeias e os Estados-Membros a:

1.3.1. zelar pela proteção da segurança e da privacidade, mediante a elaboração dos quadros regulamentares adequados, que prevejam medidas rigorosas de acompanhamento e controlo;

1.3.2. determinar claramente a responsabilidade de todos os profissionais envolvidos na cadeia de fornecimento do produto e nos fluxos de informação conexos, evitando lacunas jurídicas quando intervêm diversos produtores e distribuidores;

1.3.3. estabelecer recursos adequados e mecanismos efetivos de coordenação entre a Comissão e os Estados-Membros para garantir a aplicação coerente e harmonizada tanto da legislação revista como da nova regulamentação, tendo simultaneamente em conta o contexto internacional;

1.3.4. monitorizar o desenvolvimento das tecnologias emergentes associadas à IdC, a fim de garantir um nível elevado de segurança, a plena transparência e uma acessibilidade equitativa;

1.3.5. fomentar a normalização europeia e internacional a fim de garantir a fiabilidade, disponibilidade, resistência e manutenção dos produtos;

1.3.6. fiscalizar os mercados e preservar as condições de concorrência equitativas na implementação da IdC, evitando a concentração do poder económico transnacional nos novos intervenientes tecnológicos;

1.3.7. comprometer-se a promover ações de sensibilização e de reforço das capacidades em matéria de competências digitais, a par da investigação e da inovação de base neste domínio;

1.3.8. garantir a plena aplicação e efetiva utilização dos sistemas de resolução alternativa de litígios (RAL) e de resolução de litígios em linha (RLL);

1.3.9. incentivar a existência, a implementação e o efetivo funcionamento de um sistema europeu de ações de grupo que permita fazer cessar e também obter indemnizações sempre que a utilização da IdC cause danos ou prejuízos de natureza coletiva, como deverá decorrer do Novo Acordo para os Consumidores.

1.4. A confiança dos consumidores estará associada ao estrito cumprimento da legislação pertinente e à comunicação de boas práticas empresariais em matéria de privacidade e segurança, incumbindo às instituições integrá-las nas estratégias de responsabilidade social das empresas e nos investimentos socialmente responsáveis.

1.5. O impacto social e económico da IdC será positivo se for adequadamente associado ao desenvolvimento de políticas socioambientais no quadro da economia colaborativa, da economia circular e da economia da funcionalidade.

2. Antecedentes e contexto

2.1. Nos últimos quinze anos, o aparecimento da Internet produziu transformações em todos os domínios da vida quotidiana e teve impacto em diferentes hábitos de consumo. Por outro lado, prevê-se que, nos próximos dez anos, a revolução da Internet das coisas (IdC) chegue aos setores energético, agropecuário ou dos transportes, bem como aos setores mais tradicionais da economia e da sociedade, o que impõe a necessidade de definir políticas integrais que abordem de forma inteligente esta evolução tecnológica.

2.2. O conceito de IdC surgiu pela primeira vez no Instituto de Tecnologia de Massachusetts (MIT) e baseia-se, essencialmente, num mundo cheio de dispositivos totalmente interligados de uma forma que permita automatizar conjuntamente os diferentes processos interoperáveis. Por seu turno, a União Europeia está a preparar-se para abordar a convergência digital e os novos desafios da IdC desde o lançamento do plano «i2010 — Uma sociedade da informação europeia para o crescimento e o emprego»⁽¹⁾, até ao recente plano de ação da IdC; ver o documento «Advancing the Internet of Things in Europe» [Fazer avançar a Internet das coisas na Europa], que, em 2016, acompanhou a Comunicação da Comissão — Digitalização da Indústria Europeia — Usufruir de todos os benefícios do Mercado Único Digital⁽²⁾.

2.3. O CESE já se pronunciou em numerosas ocasiões sobre a quarta revolução industrial, marcada pela convergência de tecnologias digitais, físicas e biológicas, com destaque para o parecer de 2017⁽³⁾ sobre a matéria. Com efeito, a IdC é o terreno de eleição das formas mais avançadas de IA e onde os princípios definidos pelo CESE são postos à prova, em especial o princípio do controlo humano («human in control»).

2.4. Os dispositivos da IdC carecem, frequentemente, das normas de autenticação necessárias para garantir a segurança dos dados do utilizador. Esta situação dá origem a problemas, na medida em que deixa expostos a falhas de segurança os dispositivos, os dados e os intervenientes da cadeia de abastecimento.

2.5. As tecnologias emergentes, como a cadeia de blocos (*blockchain*), podem resolver problemas de segurança e de confiança: podem ser utilizadas para rastrear as medições dos dados provenientes de sensores, evitar a duplicação com quaisquer outros dados maliciosos e preservar a integridade e a rastreabilidade das alterações; um livro-razão distribuído pode permitir a identificação de dispositivos de IdC, a autenticação e a transferência de dados segura e sem falhas; os sensores de IdC podem ser utilizados para o intercâmbio de dados através de uma cadeia de blocos em vez de um terceiro; a utilização de contratos inteligentes permite a autonomia dos dispositivos, bem como a identidade individual e a integridade dos dados; os custos de criação e de funcionamento são reduzidos devido à ausência de intermediários; por último, os dispositivos de IdC da cadeia de blocos permitem aceder ao historial dos dispositivos ligados, o que é muito útil para a resolução de eventuais problemas⁽⁴⁾.

⁽¹⁾ COM (2005) 229 final.

⁽²⁾ COM (2016) 180 final.

⁽³⁾ Inteligência artificial — Impacto no mercado único (digital), na produção, no consumo, no emprego e na sociedade (JO C 288 de 31.8.2017, p. 1).

⁽⁴⁾ Ver Khwaja Shaik, *Why blockchain and IoT are best friends* [Por que motivo a cadeia de blocos e a IdC combinam bem], <https://www.ibm.com/us-en/?lnk=m>; sobre as inovações no setor financeiro europeu, ver JO C 246 de 28.7.2017, p. 8.

2.6. Em contrapartida, estão a ser desenvolvidas tecnologias de livro-razão distribuído de código aberto para o intercâmbio de informações e valor entre dispositivos da IdC. Estas tecnologias não permitem a prospeção de dados, mas utilizam uma arquitetura inspirada num conceito matemático designado «gráfico acíclico dirigido» (DAG), que evita as comissões e favorece o aumento da capacidade da rede em função do aumento do número de utilizadores.

2.7. Estamos perante um fenómeno com grande potencial económico ⁽⁵⁾ e social, que oferece excelentes oportunidades, mas igualmente desafios significativos com riscos implícitos, de carácter multidisciplinar e transversal e que afeta de igual modo empresas e consumidores, administrações e cidadãos. Por conseguinte, esta matéria deve ser objeto de uma abordagem comum e, simultaneamente, adequada a diversas situações específicas. A este propósito, basta referir que estimativas das Nações Unidas apontam para cinquenta mil milhões de dispositivos interligados em 2020, com aplicações para consumidores através de televisores, frigoríficos, câmaras de segurança, veículos, etc.

2.8. As aplicações da IdC estão já a gerar benefícios económicos e sociais num mundo globalizado, nomeadamente mais serviços sensíveis ao contexto socioeconómico, ciclos de retroalimentação mais curtos, reparações à distância, suportes para a tomada de decisões, melhor afetação de recursos ou o controlo remoto de serviços. Contudo, há fatores associados muito sensíveis, como a privacidade e a segurança, a assimetria da informação e a transparência das transações, responsabilidades complexas, o bloqueio de produtos e sistemas ou ainda o aumento dos produtos híbridos que pode afetar os consumidores em termos de propriedade e expô-los à aplicação de contratos à distância, que oferecem menos garantias.

2.9. Os enormes desafios jurídicos enfrentados pela UE e pelos Estados-Membros explicam-se pelo facto de muitas das características específicas da IdC (elevados níveis de complexidade e de interdependência, o elemento de autonomia, as componentes de geração e/ou tratamento de dados e uma dimensão aberta) serem comuns a outras tecnologias digitais emergentes, como a cadeia de blocos, a impressão 3D e a computação em nuvem. Na opinião do CESE, o documento de trabalho da Comissão Europeia ⁽⁶⁾ sobre a responsabilidade das tecnologias digitais emergentes constitui mais um passo na direção certa.

2.10. Por último, para maximizar os benefícios e minimizar os riscos inerentes à IdC é necessário disponibilizar informações acessíveis, claras, concisas e precisas que promovam, nomeadamente, a inclusão e a conectividade digital dos consumidores mais vulneráveis, mediante a conceção de produtos e serviços plenamente rastreáveis que comportem normas integradas de confiança, privacidade e segurança.

3. Confiança dos consumidores e dos empresários na IdC

3.1. A IdC é um ecossistema complexo que permite a interligação de dispositivos provenientes de diferentes fabricantes, distribuidores ou criadores de *software*, o que pode dificultar a determinação da responsabilidade em situações de incumprimento da regulamentação ou de danos materiais ou outros danos causados a terceiros ou a sistemas por produtos defeituosos ou por produtos utilizados abusivamente por terceiros, que não os utilizadores finais, através da rede. Aliás, é possível que muitos dos operadores que participam na cadeia de valor global do produto não possuam conhecimentos e experiência suficientes em matéria de segurança ou de proteção de dados para dispositivos em rede.

3.2. Por esse motivo, é necessária uma nova abordagem das responsabilidades que procure garantir que tanto os consumidores como as empresas que utilizam aplicações de IdC estão protegidos num ambiente em que produtos devidamente configurados podem ficar defeituosos e inseguros na sequência de incidentes de segurança digital ou de uma utilização inadequada e abusiva (por piratas informáticos, por exemplo). Esse ambiente deve permitir prever, prevenir e obter proteção contra decisões automatizadas suscetíveis de violar os princípios éticos e os direitos humanos universalmente reconhecidos.

⁽⁵⁾ A Digital McKinsey estima que, em 2025, a IdC terá um impacto económico potencial de 3 900 milhões a 11 100 milhões de dólares anuais.

⁽⁶⁾ SWD (2018) 137.

3.3. O CESE congratula-se com a revisão da aplicação da diretiva de 1985 relativa à responsabilidade decorrente dos produtos defeituosos ⁽⁷⁾, bem como com a recente criação do grupo de peritos multilateral no domínio da responsabilidade e das novas tecnologias, a fim de garantir um justo equilíbrio entre os interesses dos produtores e os dos consumidores. Um novo quadro em matéria de responsabilidade deve contemplar explicitamente a rastreabilidade da responsabilidade e da segurança, tanto ao longo da cadeia de valor do produto como durante o seu ciclo de vida, integrando a sustentabilidade como um novo fator que obrigará a considerar indispensáveis a atualização, melhoria, portabilidade, compatibilidade, reutilização, reparação ou readaptação do produto.

3.4. Deve também ser especificamente considerada para a IdC a determinação da responsabilidade de todos os profissionais envolvidos na cadeia de abastecimento do produto, evitando lacunas jurídicas quando intervêm diversos produtores e distribuidores. O CESE considera imprescindível especificar claramente os procedimentos a observar pelos consumidores em cada situação, promovendo os mecanismos de resolução alternativa de litígios (RAL).

3.5. O CESE destaca a importância da informação pré-contratual, da transparência das cláusulas contratuais e da clareza das instruções de funcionamento dos dispositivos; os riscos e os cuidados eventualmente associados devem ser devidamente salientados.

3.6. A interoperabilidade e a compatibilidade dos dispositivos e do *software* a estes associado devem ser asseguradas, a fim de evitar problemas e de permitir ao consumidor comparar fornecedores. O CESE salienta que este fator é igualmente fundamental para criar condições equitativas entre as grandes empresas e as PME.

3.7. Por último, o CESE é favorável à neutralidade da rede, pelo que insta a Comissão a assegurar um rigoroso acompanhamento do comportamento do mercado.

4. Privacidade dos consumidores na IdC

4.1. O novo Regulamento Geral de Proteção de Dados (RGPD) reforçou a capacidade dos consumidores para verificarem os seus dados pessoais e as suas preferências de privacidade ⁽⁸⁾. O utilizador de um dispositivo deve poder controlar a forma como os dados que gera são utilizados e as pessoas que podem aceder a esses dados, tendo em conta o facto de que a diversidade de dados, bem como a agregação e vinculação a outros dados, acarretam um risco grave para a privacidade no ecossistema da IdC.

4.2. Convém ter presente a incidência que a multiplicidade de produtos, serviços ou entidades pode ter na privacidade e na proteção de dados quando estes são transferidos autonomamente no contexto da sua interconectividade. Do mesmo modo, quando as informações são tratadas ou reformuladas a partir de dados inicialmente inócuos, é possível conhecer com precisão os hábitos, localização, interesses e preferências dos indivíduos, o que aumenta a acessibilidade e a rastreabilidade do perfil do utilizador.

4.3. As garantias jurídicas devem assegurar a plena capacidade dos utilizadores para exercerem o seu direito à privacidade e à proteção de dados pessoais sem qualquer limitação, evitando assim potenciais danos, como práticas discriminatórias, comercialização invasiva, perda de privacidade ou violações da segurança. Por outro lado, os consumidores devem dispor de informação sobre o valor económico dos seus dados e reservar-se o direito de os partilhar.

4.4. Conforme previsto no RGPD, as empresas e as entidades de regulamentação devem rever periodicamente o alcance da recolha de dados pessoais e avaliar em que medida os dados tratados são proporcionais e necessários para a prestação do serviço. Os aspetos e impactos de privacidade devem ser avaliados ao longo de toda a conceção, ciclo de projeto e desenvolvimento de um produto conectado e tendo em conta o ecossistema em rede em que este opera (privacidade desde a conceção). Por conseguinte, importa aplicar os princípios da privacidade desde a conceção e da privacidade predefinida de forma coerente na IdC.

4.5. Não obstante, a configuração predefinida de qualquer produto conectado deve prever o nível mais elevado de proteção da privacidade (desde a conceção e predefinida), de modo a evitar o acompanhamento indesejado do comportamento e da vida profissional dos utilizadores.

⁽⁷⁾ COM (2018) 246 final.

⁽⁸⁾ Em vigor desde 25 de maio de 2018.

4.6. Em qualquer caso, os consumidores devem dispor de informações fiáveis sobre os dados recolhidos, as pessoas que têm acesso a esses dados e a utilização que se lhes pretendem dar enquanto a relação respeitante ao produto ou serviço estiver ativa, conhecer a política de privacidade aplicável e saber se os algoritmos utilizados afetam a qualidade, o preço ou o acesso a um serviço.

5. Segurança dos consumidores e dos empresários na IdC

5.1. A interconectividade de dispositivos que caracteriza o ecossistema da IdC pode incentivar o desenvolvimento de práticas tecnológicas ilícitas ou indesejáveis que convertam este ecossistema num espaço propício a estas práticas e à sua propagação viral. Por este motivo, a segurança deve ser integral em todas e em cada uma das componentes do sistema.

5.2. A oferta de produtos e atualizações ligados à cibersegurança deve ser justificada e propor cobertura não apenas para dispositivos individuais, mas ser extensiva aos riscos de segurança inerentes à interconectividade com outros dispositivos na IdC, sem que o seu número afete negativamente os padrões de qualidade da segurança proporcionada.

5.3. Sobre esta matéria, a proposta de regulamento relativo à Agência da União Europeia para a Cibersegurança ⁽⁹⁾ prevê um quadro de certificação das tecnologias da informação e comunicação que permitirá definir mecanismos voluntários de certificação de segurança e de rotulagem para diferentes tipos de produtos, nomeadamente os da IdC. Embora se congratule com esta medida, o CESE não pode deixar de manifestar preocupação pelo facto de não ter carácter obrigatório.

5.4. As medidas de cibersegurança deveriam incluir os riscos associados a qualquer tipo de vulnerabilidade, em especial a pirataria informática e o acesso não autorizado ou uso indevido, bem como os riscos relativos aos meios de pagamento e às fraudes financeiras. A este propósito, o CESE apoia as competências atribuídas ao grupo de peritos multilateral no domínio da responsabilidade e das novas tecnologias.

5.5. Deve igualmente ser contemplada a segurança pessoal dos consumidores em relação a riscos como a utilização de proximidade, as bandas de frequência partilhadas, a exposição a campos eletromagnéticos ou a possíveis interferências com equipamentos essenciais conectados. O CESE advoga a aplicação de medidas de vigilância e a retirada preventiva em caso de riscos que afetem a saúde e a segurança dos consumidores ou os seus interesses pessoais e económicos.

5.6. As empresas devem adotar padrões de boas práticas, como a segurança desde a conceção ou predefinida, e ser submetidas a avaliações externas independentes. Em caso de incidentes de segurança ou de violações de dados, as empresas são obrigadas a notificar a ocorrência e a fornecer informações relativas à responsabilidade pelos danos e pelo incumprimento da legislação.

5.7. As empresas devem facultar aos consumidores informações simples e acessíveis, que lhes permitam tomar decisões adequadas e adotar práticas seguras, e disponibilizar-lhes as atualizações de segurança essenciais durante todo o ciclo de vida do produto.

5.8. A ausência de normas coerentes no que respeita às redes de IdC deve igualmente ser abordada. É necessário desenvolver tecnologias avançadas de banda larga e de nova geração que melhorem as infraestruturas atuais.

6. Propostas de medidas no âmbito da política pública ⁽¹⁰⁾

6.1. As autoridades públicas, no exercício dos seus poderes nos diferentes territórios da União Europeia, devem participar ativamente na elaboração das políticas e planos de ação para a IdC, com o objetivo de assegurar o equilíbrio entre as diferentes partes interessadas, antecipando as problemáticas e procurando atenuar prudencialmente os eventuais efeitos adversos. O CESE propõe:

6.1.1. a criação de ambientes de teste (*sand box*), ou seja, espaços físicos, polos, etc., para projetos-piloto e validação de conceito. Esses ambientes devem ter por objetivo testar não apenas as tecnologias, mas também os modelos de regulamentação ⁽¹¹⁾;

⁽⁹⁾ Ver documento COM (2017) 477 final.

⁽¹⁰⁾ Ver Grupo do Banco Mundial, *Internet of things: The New Government-to-Business Platform* (relatório sobre a Internet das coisas, a nova plataforma governo-empresas).

⁽¹¹⁾ Ver <https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated>

- 6.1.2. o financiamento de infraestruturas tecnológicas que permitam o desenvolvimento de projetos inovadores de IdC no âmbito do novo programa Horizonte Europa;
- 6.1.3. a designação de institutos e agências independentes como facilitadores e supervisores dos projetos de IdC. O CESE congratula-se com as medidas pertinentes previstas no regulamento relativo à cibersegurança de 2017 e exorta a Comissão a promover efetivamente processos de normalização na indústria digital, disponibilizando, para o efeito, recursos orçamentais adequados ⁽¹²⁾;
- 6.1.4. a promoção de associações e plataformas de colaboração público-privadas que envolvam a comunidade científica, a indústria e os consumidores;
- 6.1.5. o fomento do investimento no desenvolvimento de modelos empresariais locais que tirem partido dos benefícios da IdC e facilitem a abordagem de aspetos tão complexos como a proteção e a propriedade dos dados;
- 6.1.6. a realização de ações de reforço das capacidades no âmbito empresarial, na perspetiva da corresponsabilidade. Importa garantir a integração da segurança e da privacidade desde a conceção e predefinida nos produtos e serviços das TIC, em conformidade com o «dever de diligência» defendido no novo regulamento sobre cibersegurança. Neste contexto, o CESE saúda a prevista elaboração de **códigos de conduta** destinados a complementar o regulamento;
- 6.1.7. o fomento das iniciativas de normalização europeias e internacionais que visem garantir que os sistemas de IdC possuem as características essenciais, a saber, fiabilidade, segurança, disponibilidade, resistência, possibilidade de manutenção e utilização. Nomeadamente, a normalização é fundamental para a rápida execução de processos de fabrico industrial altamente digitalizados;
- 6.1.8. a garantia de que os utilizadores da IdC, sobretudo os mais vulneráveis e os que vivem em zonas pouco povoadas, dispõem de acesso de alta qualidade e a preços razoáveis;
- 6.1.9. a promoção de campanhas de sensibilização e de programas educativos destinados a facilitar a adoção da IdC por parte das empresas e dos consumidores, proporcionando-lhes a possibilidade de adquirir as capacidades e competências necessárias ⁽¹³⁾, prestando particular atenção aos grupos vulneráveis e à diversidade;
- 6.1.10. o lançamento de iniciativas de caráter educativo com vista a uma prevenção adequada, atenta a integração precoce da população infantil em ambientes digitais;
- 6.1.11. o lançamento de análises de diagnóstico e de estudos do impacto da IdC em domínios como os novos modelos de produção e consumo sustentáveis;
- 6.1.12. a garantia da plena aplicação e efetiva utilização dos sistemas de resolução alternativa de litígios (RAL) e de resolução de litígios em linha (RLL);
- 6.1.13. incentivar a existência, a implementação e o efetivo funcionamento de um sistema europeu de ações de grupo que permita fazer cessar e também obter indemnizações sempre que a utilização da IdC cause danos ou prejuízos de natureza coletiva, como deverá decorrer do Novo Acordo para os Consumidores.
- 6.2. O CESE insta ainda a Comissão a avaliar as regras direta ou indiretamente relacionadas com a IdC e, se necessário, a melhorar a legislação em vigor. Neste contexto, o **Novo Acordo para os Consumidores** deve centrar-se igualmente nos dispositivos que se conectam, nas redes e na segurança das mesmas, bem como nos dados associados aos dispositivos.
- 6.3. Por último, o CESE salienta a importância do estabelecimento de mecanismos de cooperação e de coordenação entre os Estados-Membros, com vista a uma aplicação eficiente e uniforme da regulamentação, bem como dos acordos que a União Europeia venha a celebrar no exterior do seu território devido à localização das sedes de empresas e fornecedores, com particular ênfase no intercâmbio de boas práticas. A política internacional em matéria de fluxos transfronteiriços de dados deve ser coordenada, de modo que os países em causa possam estabelecer normas de proteção igualmente elevadas nas respetivas legislações nacionais, tanto substantivas como processuais.

Bruxelas, 19 de setembro de 2018.

O Presidente
do Comité Económico e Social Europeu
Luca JAHIER

⁽¹²⁾ JO C 197 de 8.6.2018, p. 17.

⁽¹³⁾ JO C 434 de 15.12.2017, p. 36.