Translations proofread by EDPB Members.
This language version has not yet been proofread.

Declaração 03/2021 sobre o Regulamento Privacidade Eletrónica

Adotada em 9 de março de 2021

O Comité Europeu para a Proteção de Dados adotou a seguinte declaração:

O CEPD congratula-se com o acordo sobre o mandato de negociação adotado pelo Conselho relativo à proteção da privacidade e da confidencialidade na utilização de serviços de comunicações eletrónicas (a seguir designado «posição do Conselho»), que considera um passo positivo no sentido de um novo Regulamento Privacidade Eletrónica. É muito importante que o quadro geral da UE em matéria de proteção de dados seja rapidamente complementado com regras harmonizadas para as comunicações eletrónicas.

Como já referido em várias ocasiões[1], o Regulamento Privacidade Eletrónica não deve, em caso algum, reduzir o nível de proteção proporcionado pela atual Diretiva Privacidade Eletrónica, devendo antes complementar o RGPD, proporcionando garantias adicionais sólidas de confidencialidade e proteção para todos os tipos de comunicações eletrónicas. O Regulamento Privacidade Eletrónica não pode, de modo algum, ser utilizado para alterar de facto o RGPD. A este respeito, a posição do Conselho suscita uma série de preocupações e o CEPD deseja chamar a atenção para questões que deverão ser abordadas nas próximas negociações.

A presente declaração não prejudica eventuais futuras declarações ou pareceres mais pormenorizados do CEPD sobre as posições dos colegisladores.

[1] Ver a lista completa de documentos sobre as regras em matéria de privacidade e comunicações eletrónicas elaborada pelo CEPD e pelo Grupo de Trabalho do artigo 29.º como anexo à presente declaração.

Preocupações relativas ao tratamento e conservação de dados de comunicações eletrónicas para efeitos de aplicação da lei e de salvaguarda da segurança nacional

No que diz respeito ao artigo 6.º, n.º 1, alínea d), e ao artigo 7.º, n.º 4, o CEPD reitera que as medidas legislativas que exigem aos prestadores de serviços de comunicações eletrónicas que conservem dados de comunicações eletrónicas têm de respeitar:

- Os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE (a «Carta»),
- A jurisprudência mais recente do Tribunal de Justiça da UE (o «TJUE»)[2], bem como
- O Artigo 8.º da Convenção Europeia dos Direitos Humanos.

O CEPD considera que o Regulamento Privacidade Eletrónica não pode derrogar a aplicação da jurisprudência mais recente do TJUE, segundo a qual, nomeadamente, os artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta devem ser interpretados no sentido de que proíbem medidas legislativas que imponham, como medida preventiva, a conservação geral e indiscriminada dos dados de tráfego e de localização. Por conseguinte, a Carta não permite uma base jurídica que preveja uma conservação não seletiva para efeitos de aplicação da lei e de salvaguarda da segurança nacional, que deve, de qualquer modo, estar sujeita a limitações temporais e materiais rigorosas, bem como a controlo por parte de um tribunal ou uma autoridade independente.

Quanto à exclusão das atividades de tratamento dos prestadores do âmbito de aplicação do regulamento, o CEPD considera que essa exclusão é contrária à premissa de um quadro coerente da UE em matéria de proteção de dados. O CEPD salienta que, no entanto, em caso de exclusão, o RGPD é aplicável.

A confidencialidade das comunicações eletrónicas exige proteção específica (artigos 6.º, 6.º-A, 6.º-B e 6.º-C)

A confidencialidade das comunicações é um direito fundamental protegido pelo artigo 7.º da Carta e já aplicado pela Diretiva Privacidade Eletrónica. Este direito à confidencialidade deve ser aplicado a todas as comunicações eletrónicas, independentemente do meio através do qual são enviadas, em repouso e em trânsito, do remetente ao destinatário, e deve também proteger a integridade de todo o equipamento terminal do utilizador.

Proibições gerais com exceções estritas para o tratamento de dados pessoais

O CEPD apoia plenamente a abordagem baseada em proibições gerais e com exceções estritas, específicas e claramente definidas (em função da finalidade).

No entanto, o CEPD vê com receio que algumas exceções introduzidas pelo Conselho (em especial o artigo 6.º, n.º 1, alínea c), o artigo 6.º-B, n.º 1, alínea e), o artigo 6.º-B, n.º 1, alínea f), e o artigo 6.º-C) parecem permitir tipos de tratamento muito amplos, e recorda a necessidade de limitar essas exceções a finalidades específicas e claramente definidas. Em qualquer caso, esses objetivos específicos devem ser explicitamente enumerados, a fim de garantir a segurança jurídica e o mais elevado grau possível de proteção.

Além disso, as exceções previstas no artigo 6.º, n.º 1, alínea b), alínea c), e alínea d), que permitem o acesso a dados de comunicações eletrónicas, incluindo conteúdos, para garantir a segurança da rede e dos dispositivos do utilizador final, podem permitir o pleno acesso do prestador de serviços de comunicações eletrónicas ou dos seus subcontratantes ao conteúdo de todas as comunicações dos utilizadores finais. Dado que tal pode comprometer as expectativas do utilizador final em matéria de

[2] TJUE, processos apensos C-511/18, C-512/18 e C-520/18, processo C-623/17.

direito à privacidade e confidencialidade, é necessário assegurar a sua proporcionalidade e restringir o seu uso, pelo menos para recordar que tal não pode conduzir à monitorização sistemática do conteúdo das comunicações eletrónicas, nem permitir que os fornecedores ou subcontratantes contornem qualquer cifragem.

Por último, o regulamento deve salientar o papel da anonimização como garantia fundamental que deve ser sistematicamente favorecida no que diz respeito à utilização de dados de comunicações eletrónicas.

A disponibilidade de uma cifragem forte e fidedigna é uma necessidade no mundo digital moderno.

A cifragem forte e atualizada deve ser a regra geral para garantir um fluxo seguro, livre e fiável de dados entre os cidadãos, as empresas e os governos, e é crucial para garantir o cumprimento da obrigação de segurança prevista no RGPD, por exemplo, para os dados de saúde e a proteção dos sistemas informáticos num contexto de ameaças crescentes. A cifragem de ponta a ponta, desde o remetente até ao destinatário, é também a única forma de assegurar a plena proteção dos dados em trânsito. Qualquer tentativa de enfraquecimento da cifragem, mesmo para fins como a segurança nacional, esvaziaria completamente esses mecanismos de proteção devido à sua possível utilização ilícita. A cifragem deve continuar a ser normalizada, forte e eficiente[3].

O novo regulamento deve aplicar o requisito relativo ao consentimento para os testemunhos de conexão (*cookies*) e as tecnologias semelhantes e proporcionar aos prestadores de serviços os meios técnicos que lhes permitam obter esse consentimento (artigo 8.º[4])

A necessidade de uma abordagem que preserve a privacidade relativamente às soluções do tipo «pegar ou largar»

Importa recordar que as disposições do GPDR relativas ao consentimento são aplicáveis no contexto das regras relativas à privacidade das comunicações eletrónicas. Por conseguinte, o CEPD considera que a necessidade de obter um consentimento genuinamente livre deve impedir os prestadores de serviços de recorrerem a práticas desleais, como soluções de «pegar ou largar», que condicionam o acesso a serviços e funcionalidades ao consentimento de um utilizador para o armazenamento de informações ou à obtenção de acesso a informações já armazenadas no equipamento terminal de um utilizador (as chamadas «barreiras de testemunhos de conexão» ou «*cookie walls*»)[5].

O CEPD salienta a necessidade de incluir uma disposição explícita no Regulamento Privacidade Eletrónica para consagrar esta proibição, de forma a permitir que os utilizadores aceitem ou recusem a definição de perfis. Por conseguinte, devem ser propostas aos utilizadores alternativas justas oferecidas pelos mesmos prestadores de serviços. Esses princípios deverão aplicar-se igualmente a todos os prestadores de serviços, independentemente do seu setor de atividade ou do seu atual modelo de financiamento (ver considerando 21-AA da posição do Conselho).

---

3 Declaração do Grupo de Trabalho do artigo 29.º sobre a cifragem e o seu impacto na proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais na UE, de 11 de abril de 2018, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

4 Bem como os considerandos conexos (20-AAAA e 21-AA da posição do Conselho).

5 Tal como referido anteriormente pelo CEPD na Declaração sobre a revisão do Regulamento Privacidade Eletrónica, adotada em 25 de maio de 2018, disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf e nas Diretrizes 05/2019 do CEPD relativas ao consentimento na aceção do Regulamento 2016/679, ponto 39, disponíveis em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_pt.pdf.

A medição das audiências deve limitar-se a práticas não intrusivas que não possam constituir um risco para a privacidade para os utilizadores

A posição do Conselho cria uma nova exceção para a medição das audiências, tal como sugerido pelo Grupo de Trabalho do artigo 29.º[6]. No entanto, a derrogação para a medição de audiências proposta pelo Conselho está formulada de forma demasiado ampla e pode conduzir a uma interpretação excessivamente lata do que poderia ser abrangido pelo seu âmbito de aplicação e, consequentemente, reduzir o nível de proteção dos terminais dos utilizadores finais.

Por conseguinte, o CEPD salienta que a derrogação para a medição de audiências deve limitar-se a análises de baixo nível necessárias para o estudo do desempenho do serviço solicitado pelo utilizador e deve limitar-se exclusivamente ao fornecimento de estatísticas ao operador de serviços, devendo ser posta em prática pelo operador ou pelos seus subcontratantes. Com efeito, esta operação de tratamento não pode dar origem, por si só ou em combinação com outras soluções de rastreio, a qualquer seleção ou definição de perfis dos utilizadores pelo fornecedor ou por outros responsáveis pelo tratamento de dados. Além disso, o serviço de medição de audiências não deve permitir a recolha de informações sobre navegação dos utilizadores em diferentes sítios Web/aplicações e deve incluir um mecanismo facilmente acessível de autoexclusão de qualquer recolha de dados.

Forma eficaz de obter consentimento para sítios Web e aplicações móveis (artigo 4.º-A)

O CEPD considera que o Regulamento Privacidade Eletrónica deve melhorar a situação atual, devolvendo o controlo aos utilizadores e abordando o «cansaço do consentimento». O artigo 4.º-A deve ir mais longe e obrigar os programas de navegação e os sistemas operativos a criar um mecanismo eficaz e facilmente acessível que permita aos responsáveis pelo tratamento obter o consentimento, a fim de criar condições equitativas entre todos os intervenientes. O âmbito de aplicação do regulamento deve também incluir explicitamente os fornecedores de programas de navegação e de sistemas operativos.

As predefinições de privacidade devem preservar o direito à proteção dos dados pessoais e a integridade dos terminais dos utilizadores por defeito e facilitar a expressão e a retirada do consentimento de uma forma fácil, vinculativa e oponível a todas as partes.

Tratamento posterior para finalidades compatíveis (artigo 6.º-C artigo 8.º, n.º 1, alínea g),)

Em relação aos debates em curso sobre o tratamento posterior dos metadados/dados das comunicações eletrónicas recolhidos através de testemunhos de conexão e tecnologias semelhantes, o CEPD reitera o seu apoio à abordagem do Regulamento Privacidade Eletrónica, tal como inicialmente proposto pela Comissão Europeia e seguido pelo Parlamento Europeu, com base numa proibição geral, seguido de exceções restritivas e da utilização do consentimento. O tratamento posterior para finalidades compatíveis comporta o risco de comprometer a proteção conferida pelo Regulamento Privacidade Eletrónica, especialmente no tratamento de metadados de comunicações eletrónicas, ao permitir o tratamento para qualquer finalidade que o prestador de serviços considere cumprir a cláusula de «compatibilidade», apesar de o legislador ter claramente procurado restringir a sua utilização a finalidades específicas na ausência de consentimento. O CEPD gostaria de salientar que os dados acima referidos podem continuar a ser tratados sem consentimento e sem criar riscos para os utilizadores após terem sido anonimizados.

---

[6] Ver também o Parecer 04/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão (WP 194), pontos 10 e 11. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf.

Futuro papel das autoridades de controlo, do CEPD e do mecanismo de cooperação (artigos 18.º a 20.º)

O CEPD recorda que, a fim de garantir condições de concorrência equitativas no mercado único digital, é essencial assegurar uma interpretação e aplicação harmonizadas de todas as disposições relativas ao tratamento de dados do Regulamento Privacidade Eletrónica em toda a UE.

A fim de reforçar a coerência, a supervisão das disposições em matéria de privacidade nos termos do Regulamento Privacidade Eletrónica deve ser confiada às autoridades de controlo competentes ao abrigo do RGPD

O CEPD gostaria de recordar que existe uma clara interligação entre as competências das autoridades nacionais competentes ao abrigo da atual Diretiva Privacidade Eletrónica e as autoridades de proteção de dados. As disposições do futuro Regulamento Privacidade Eletrónica relacionadas com a proteção da privacidade não devem ser aplicadas isoladamente, uma vez que estão interligadas com o tratamento de dados pessoais e com o RGPD.

Por conseguinte, a fim de conciliar um elevado nível de proteção dos dados pessoais e a segurança jurídica e processual, as autoridades nacionais responsáveis pela aplicação do RGPD devem ser incumbidas da supervisão das disposições do futuro Regulamento Privacidade Eletrónica relacionadas com o tratamento de dados pessoais, tal como inicialmente proposto pela Comissão Europeia[7].

O CEPD observa que, ao contrário da proposta inicial da Comissão Europeia, todas as referências ao mecanismo de cooperação e de controlo da coerência previstas no capítulo VII do RGPD foram retiradas da posição do Conselho. Pelas razões acima referidas, o CEPD reitera que só um alinhamento perfeito com o quadro de cooperação e coerência do RGPD permitiria ao Regulamento Privacidade Eletrónica alcançar os seus objetivos, evitar a fragmentação na sua aplicação e execução, bem como reduzir os encargos para os prestadores que, de outra forma, teriam de se dirigir a mais de 27 autoridades de controlo.

No caso de as autoridades nacionais competentes que não são membros do CEPD terem de interagir com o CEPD, como atualmente prevê a posição do Conselho, a sua capacidade de contribuir atempadamente para uma aplicação coerente do Regulamento Privacidade Eletrónica diminuiria em detrimento tanto da economia digital como da proteção dos direitos fundamentais.

Pelo Comité Europeu para a Proteção de Dados

Presidente

(Andrea Jelinek)

[7] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), de 10 de janeiro de 2017, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010, e o parecer associado do Grupo de Trabalho do artigo 29.º, disponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

ANEXO: Lista de documentos anteriores elaborados pelo CEPD e pelo Grupo de Trabalho do artigo 29.º

- Parecer 1/2009 sobre as propostas que alteram a Diretiva 2002/58/CE relativa à privacidade e às comunicações eletrónicas (Diretiva Privacidade Eletrónica), disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_pt.pdf.
- Parecer 04/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão (WP 194), disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_pt.pdf.
- Parecer 03/2016 sobre a avaliação e revisão da Diretiva Privacidade Eletrónica (WP 240), disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
- Parecer do Grupo de Trabalho do artigo 29.º sobre a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas), disponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
- Declaração do Grupo de Trabalho do artigo 29.º sobre a cifragem e o seu impacto na proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais na UE, Bruxelas, 11 de abril de 2018, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
- Declaração do CEPD sobre a revisão do Regulamento Privacidade Eletrónica e o seu impacto na proteção das pessoas singulares no que diz respeito à privacidade e confidencialidade das suas comunicações, adotada em 25 de maio de 2018, disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.
- Declaração 3/2019 do CEPD sobre um regulamento relativo à privacidade e às comunicações eletrónicas, adotada em 13 de março de 2019, disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf.
- Declaração do CEPD sobre o Regulamento Privacidade Eletrónica e o futuro papel das autoridades de controlo e do CEPD, adotada em 19 de novembro de 2020, disponível em: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_pt.