

(Atos legislativos)

I

REGULAMENTOS

REGULAMENTO (UE) 2022/1925 DO PARLAMENTO EUROPEU E DO CONSELHO

14 de setembro de 2022

sobre mercados contestáveis e justos no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais)

(Texto relevante para o EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após a transmissão do projecto de acto legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ⁽¹⁾,

Tendo em conta o parecer do Comité das Regiões ⁽²⁾,

De acordo com o processo legislativo ordinário ⁽³⁾,

Considerando o seguinte:

(1) Os serviços digitais em geral e as plataformas em linha em particular desempenham um papel cada vez mais importante importante para a economia, especialmente no mercado interno, ao permitir que as empresas cheguem aos utilizadores em toda a União, facilitando o comércio transfronteiriço e oferecendo oportunidades de negócio completamente novas a um grande número de empresas na União, em benefício dos consumidores da União.

(2) Ao mesmo tempo, entre estes serviços digitais, os serviços básicos de plataforma apresentam uma série de características que podem ser aproveitadas pelas empresas que os prestam. Um exemplo desses recursos dos principais serviços de plataforma são as economias de escala extremas, que geralmente resultam dos custos marginais quase nulos de adição de usuários comerciais ou finais. Outras características semelhantes dos serviços básicos de plataforma são efeitos de rede muito poderosos e a capacidade de conectar muitos usuários profissionais com muitos usuários finais graças ao caráter multilateral.

⁽¹⁾ DO C 286 de 16.7.2021, p. 64. ⁽²⁾

DO C 440 de 29.10.2021, p. 67.

⁽³⁾ Posição do Parlamento Europeu de 5 de julho de 2022 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 18 de julho de 2022.

desses serviços, um grau significativo de dependência de usuários profissionais e usuários finais, efeitos de bloqueio, falta de multiconexão para o mesmo propósito por usuários finais, integração vertical e vantagens derivadas de dados. Todas essas características, combinadas com práticas desleais de empresas que fornecem serviços básicos de plataforma, podem ter o efeito de prejudicar substancialmente a contestabilidade dos serviços básicos de plataforma, bem como afetar a imparcialidade do relacionamento comercial entre as empresas que fornecem tais serviços e seus usuários profissionais e usuários finais. Na prática, isto leva a uma redução rápida e potencialmente extensa na escolha para empresas e utilizadores finais e pode, portanto, dar ao fornecedor de tais serviços a posição de “guardião”. Ao mesmo tempo, deve reconhecer-se que os serviços que operam para fins não comerciais, como projetos colaborativos, não devem ser considerados serviços essenciais de plataforma para efeitos do presente regulamento.

- (3) Um pequeno número de grandes empresas que prestam serviços essenciais de plataforma acumularam poder económico significativo, o que as pode qualificar para serem designadas como controladoras de acesso ao abrigo do presente regulamento. Eles normalmente têm a capacidade de conectar muitos usuários empresariais a muitos usuários finais por meio de seus serviços, o que, por sua vez, lhes permite transferir seus benefícios, como acesso a grandes quantidades de dados, de uma área de atividade para outra. Algumas dessas empresas controlam ecossistemas inteiros de plataformas na economia digital, e os operadores de mercado existentes ou novos, não importa o quão inovadores e eficientes sejam, acham extremamente difícil, por razões estruturais, competir com elas ou desafiar sua participação de mercado. A contestabilidade é reduzida, em particular, pela existência de enormes barreiras à entrada ou saída do mercado, como altos custos de investimento, que não podem ser recuperados, ou pelo menos não facilmente, em caso de saída, e a ausência ou acesso limitado a alguns insumos essenciais na economia digital, como dados. Como resultado, a probabilidade de que os mercados subjacentes não tenham um bom desempenho ou parem de ter um bom desempenho em breve aumenta.
- (4) A combinação destas características dos controladores de acesso é susceptível de conduzir, em muitos casos, a graves desequilíbrios no poder de negociação e, conseqüentemente, a práticas e condições desleais para os utilizadores empresariais, bem como para os utilizadores finais dos principais serviços de plataforma fornecidos pelos controladores de acesso, em detrimento dos preços, da qualidade, da concorrência leal, da escolha e da inovação no sector digital.
- (5) Daqui decorre que a dinâmica do mercado é muitas vezes incapaz de garantir resultados económicos justos no que diz respeito aos principais serviços de plataforma. Embora os artigos 101 e 102 do Tratado sobre o Funcionamento da União Europeia (TFUE) se apliquem à conduta dos controladores de acesso, o âmbito dessas disposições é limitado a certos casos de poder de mercado (por exemplo, domínio em mercados específicos) e comportamento anticompetitivo, e o controle de conformidade ocorre ex post e requer uma investigação extensiva, caso a caso, de fatos muitas vezes muito complexos. Além disso, a legislação atual da União não aborda, ou pelo menos não de forma eficaz, os desafios ao funcionamento eficiente do mercado interno colocados pela conduta de controladores de acesso que não são necessariamente dominantes em termos de direito da concorrência.
- (6) Os controladores de acesso têm uma influência importante no mercado interno, uma vez que fornecem portas de entrada para um grande número de utilizadores profissionais chegarem aos utilizadores finais em qualquer lugar da União e em diferentes mercados. O impacto negativo de práticas desleais no mercado interno e a baixa contestabilidade dos principais serviços de plataforma, incluindo as consequências sociais e económicas negativas dessas práticas desleais, levaram legisladores nacionais e reguladores do setor a agir. Várias soluções regulatórias já foram adotadas ou propostas em nível nacional para abordar práticas desleais e contestabilidade de serviços digitais, ou pelo menos com relação a algumas delas. Isso criou soluções regulatórias divergentes, levando à fragmentação do mercado interno e, portanto, aumentando o risco de maiores custos de conformidade devido à existência de diferentes conjuntos de requisitos regulatórios nacionais.
- (7) Por conseguinte, o objetivo do presente regulamento é contribuir para o bom funcionamento do mercado interno, estabelecendo regras que assegurem a disputabilidade e a equidade dos mercados no setor digital em geral e assegurá-las para os utilizadores profissionais e os utilizadores finais de serviços básicos de plataforma prestados por controladores de acesso em particular. Os usuários empresariais e os usuários finais dos principais serviços de plataforma fornecidos pelos controladores de acesso devem receber salvaguardas regulatórias adequadas em toda a União contra práticas desleais dos controladores de acesso, a fim de facilitar as atividades comerciais.

transações transfronteiriças na União, melhorando assim o bom funcionamento do mercado interno e eliminando a fragmentação que existe ou pode surgir nos domínios específicos aos quais o presente regulamento se aplica. Além disso, embora os gatekeepers tendam a adotar modelos de negócios e estruturas algorítmicas globais ou pelo menos pan-europeus, eles também podem, e em alguns casos já adotaram, diferentes condições e práticas comerciais em diferentes Estados-Membros, o que pode criar disparidades entre as condições de concorrência para os usuários dos principais serviços de plataforma fornecidos pelos gatekeepers, em detrimento da integração do mercado interno.

(8) Ao aproximar as legislações nacionais divergentes, é possível eliminar os obstáculos à liberdade de prestar e receber serviços, incluindo serviços de retalho, no mercado interno. Por conseguinte, deve ser estabelecido um conjunto harmonizado de obrigações legais a nível da União para garantir a disputabilidade e a equidade dos mercados digitais, com a presença de controladores no mercado interno, em benefício da economia da União como um todo e, em última análise, dos consumidores da União.

(9) A fragmentação do mercado interno só pode ser eficazmente evitada se os Estados-Membros forem impedidos de aplicar regras nacionais abrangidas pelo âmbito de aplicação do presente regulamento e que prossigam os mesmos objetivos. Isto não exclui a possibilidade de que outras regras nacionais que prossigam outros objetivos legítimos de interesse público, conforme estabelecido no TFUE, ou razões imperiosas de interesse geral reconhecidas na jurisprudência do Tribunal de Justiça da União Europeia (doravante «Tribunal de Justiça»), possam ser aplicadas aos controladores de acesso na aceção do presente regulamento.

(10) Ao mesmo tempo, uma vez que o presente regulamento se destina a complementar a aplicação do direito da concorrência, deverá aplicar-se sem prejuízo dos artigos 101.º e 102.º do TFUE, das regras nacionais de concorrência aplicáveis e de outras regras nacionais de concorrência relativas a condutas unilaterais baseadas numa avaliação individualizada das posições e do comportamento no mercado, incluindo os seus efeitos reais ou potenciais e o âmbito preciso da conduta proibida, e prevendo a possibilidade de as empresas apresentarem justificações fundamentadas quanto à eficiência e aos objetivos da conduta em questão, bem como às regras nacionais em matéria de controlo de concentrações. Contudo, a aplicação dessas regras não deverá afetar as obrigações impostas aos controladores de acesso ao abrigo do presente regulamento nem a sua aplicação uniforme e efetiva no mercado interno.

(11) Os artigos 101.º e 102.º do TFUE e as correspondentes regras nacionais de concorrência relativas a condutas anticoncorrenciais multilaterais e unilaterais e ao controlo das concentrações visam proteger a concorrência não distorcida no mercado. O presente regulamento persegue um objetivo complementar, mas distinto, ao de proteger a concorrência não distorcida num determinado mercado, tal como definido no direito da concorrência, que consiste em garantir que os mercados em que os controladores de acesso estão presentes sejam e permaneçam contestáveis e justos, independentemente dos efeitos reais, potenciais ou suspeitos sobre a concorrência num determinado mercado da conduta de um controlador de acesso específico ao qual o presente regulamento se aplica. O presente regulamento visa, portanto, proteger um interesse jurídico diferente daquele protegido por essas regras e deverá aplicar-se sem prejuízo da aplicação destas últimas.

(12) O presente regulamento deverá também aplicar-se sem prejuízo das regras decorrentes de outros atos do direito da União que regulam determinados aspetos da prestação de serviços abrangidos pelo âmbito de aplicação do presente regulamento, em especial o Regulamento (UE) 2016/679 (4) e (UE) 2019/1150 (5) do Parlamento Europeu e da

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

(5) Regulamento (UE) 2019/1150 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha (JO L 186 de 11.7.2019, p. 57).

Conselho e um regulamento sobre um mercado único para os serviços digitais, e a Directiva 2002/58/CE ⁽⁶⁾, 2005/29/CE ⁽⁷⁾, 2010/13/UE ⁽⁸⁾, (UE) 2015/2366 ⁽⁹⁾, (UE) 2019/790 ⁽¹⁰⁾ e (UE) 2019/882 ⁽¹¹⁾ do Parlamento Europeu e do Conselho, e a Directiva 93/13/CEE ⁽¹²⁾ do Conselho e das normas nacionais de execução desses atos da União.

(13) A baixa contestabilidade e as práticas desleais no setor digital são mais frequentes e pronunciadas para alguns serviços digitais do que para outros. Eles afetam particularmente serviços digitais amplamente difundidos e comumente usados, que servem principalmente como intermediários diretos entre usuários empresariais e usuários finais e, mais frequentemente, apresentam características como economias de escala extremas, efeitos de rede muito fortes, capacidade de conectar muitos usuários empresariais com muitos usuários finais graças à natureza multilateral dos serviços, efeitos de bloqueio, falta de multiconexão ou integração vertical. Muitas vezes, esses serviços digitais são fornecidos por uma única grande empresa ou por um número muito pequeno de grandes empresas. Na maioria das vezes, essas empresas se estabeleceram como guardiãs para empresas e usuários finais, com repercussões de longo alcance. Em particular, eles adquiriram a capacidade de definir facilmente condições comerciais de forma unilateral e prejudicial para seus usuários comerciais e usuários finais. Portanto, é necessário focar apenas nos serviços digitais mais amplamente utilizados por empresas e usuários finais e para os quais as preocupações com baixa contestabilidade e práticas injustas de controle são mais evidentes e urgentes de uma perspectiva de mercado interno.

(14) Em particular, os serviços de intermediação em linha, os motores de busca em linha, os sistemas operativos, as redes sociais em linha, os serviços de plataformas de partilha de vídeos, os serviços de comunicações interpessoais independentes de números, os serviços de computação em nuvem, os assistentes virtuais, os navegadores da Web e os serviços de publicidade em linha, incluindo os serviços de intermediação de publicidade, têm o potencial de afectar um grande número de utilizadores finais e de empresas, conduzindo ao risco de práticas comerciais desleais. Devem, portanto, ser incluídos na definição de serviços essenciais de plataforma e enquadrar-se no âmbito do presente regulamento. Os serviços de intermediação em linha também podem desempenhar um papel no domínio dos serviços financeiros e podem atuar como intermediários ou ser utilizados para fornecer os serviços enumerados de forma não exaustiva no Anexo II da Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho ⁽¹³⁾. Para efeitos do presente regulamento, a definição de serviços essenciais de plataforma deverá ser neutra em termos de tecnologia e deverá ser entendida como incluindo serviços prestados em ou através de vários meios ou dispositivos, como televisores inteligentes ou serviços digitais a bordo dos veículos. Em certas circunstâncias, o conceito de usuários finais deve incluir usuários que são tradicionalmente considerados usuários empresariais, mas que em certas situações não usam os serviços principais da plataforma para fornecer produtos ou serviços a outros usuários finais, como empresas que dependem de serviços de computação em nuvem para seus próprios propósitos.

⁽⁶⁾ Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Directiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

⁽⁷⁾ Directiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Directiva 84/450/CEE do Conselho, as Directivas 97/7/CE, 98/27/CE e 2002/65/CE do Parlamento Europeu e do Conselho e o Regulamento (CE) n.º 1017/2005, qualquer 2006/2004 do Parlamento Europeu e do Conselho («Directiva relativa às práticas comerciais desleais») (JO L 149 de 11.6.2005, p. 22).

⁽⁸⁾ Directiva 2010/13/UE do Parlamento Europeu e do Conselho, de 10 de março de 2010, relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Directiva Serviços de Comunicação Social Audiovisual) (JO L 95 de 15.4.2010, p. 1).

⁽⁹⁾ Directiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno e que altera as Directivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1079/2015, qualquer 1093/2010 e que revoga a Directiva 2007/64/CE (JO L 337 de 23.12.2015, p. 35).

⁽¹⁰⁾ Directiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Directivas 96/9/CE e 2001/29/CE (JO L 130 de 17.5.2019, p. 92).

⁽¹¹⁾ Directiva (UE) 2019/882 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos requisitos de acessibilidade dos produtos e serviços (JO L 151 de 7.6.2019, p. 70).

⁽¹²⁾ Directiva 93/13/CEE do Conselho, de 5 de Abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores (JO L 95 de 21.4.1993, p. 29).

⁽¹³⁾ Directiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

(15) O facto de um serviço digital ser um serviço de plataforma básico não suscita, por si só, preocupações suficientemente sérias em termos de contestabilidade ou de práticas desleais. Tais preocupações surgem apenas quando um serviço de plataforma principal constitui um gateway importante e é operado por uma empresa com influência significativa no mercado doméstico e uma posição estabelecida e de longa data, ou uma empresa que deve desfrutar de tal posição em um futuro próximo. Por conseguinte, o conjunto específico de regras harmonizadas previsto no presente regulamento deverá aplicar-se apenas às empresas designadas com base nesses três critérios objetivos e deverá aplicar-se apenas aos principais serviços de plataforma dessas empresas que, individualmente, constituem uma importante porta de entrada para os utilizadores empresariais chegarem aos utilizadores finais. O fato de ser possível para um provedor de serviços de plataforma central mediar não apenas entre usuários empresariais e usuários finais, mas também entre usuários finais e usuários finais (por exemplo, no caso de serviços de comunicações interpessoais independentes de número) não deve impedir a conclusão de que tal provedor é ou pode ser uma porta de entrada importante para usuários empresariais alcançarem usuários finais.

(16) A fim de assegurar a aplicação efetiva do presente regulamento às empresas que prestam serviços essenciais de plataforma com maior probabilidade de satisfazer esses requisitos objetivos, e nos casos em que as práticas desleais que reduzem a disputabilidade são mais generalizadas e têm maior impacto, a Comissão deverá poder designar diretamente como controladores de acesso as empresas que prestam serviços essenciais de plataforma que cumprem determinados limiares quantitativos. Em qualquer caso, essas empresas devem passar por um procedimento de designação rápida que deve ter início assim que o presente regulamento se tornar aplicável.

(17) O facto de uma empresa ter um grande volume de negócios na União e prestar um serviço de plataforma essencial em pelo menos três Estados-Membros constitui uma indicação convincente de que essa empresa tem uma influência significativa no mercado interno. Isto é igualmente verdade quando uma empresa que fornece um serviço de plataforma essencial em pelo menos três Estados-Membros tem uma capitalização de mercado muito elevada ou um valor justo de mercado equivalente. Por conseguinte, deve presumir-se que uma empresa que fornece um serviço essencial de plataforma tem uma influência significativa no mercado interno quando fornece um serviço essencial de plataforma em pelo menos três Estados-Membros e quando o volume de negócios alcançado pelo seu grupo na União é igual ou excede um determinado limiar elevado, ou quando a capitalização bolsista do grupo é igual ou excede um determinado valor absoluto elevado. Para empresas que prestam serviços básicos de plataforma e que pertencem a empresas não listadas em um mercado regulamentado, o valor justo de mercado equivalente deve ser tomado como referência. A Comissão deve poder usar os seus poderes para adotar atos delegados para desenvolver uma metodologia objetiva para calcular esse valor.

Um alto volume de negócios de um grupo obtido na União, juntamente com um número de usuários de serviços básicos de plataforma na União igual ao limite, reflete uma capacidade relativamente grande de monetizar esses usuários. Uma alta capitalização de mercado em relação ao mesmo número de usuários na União reflete um potencial relativamente grande de monetização desses usuários em um futuro próximo. Esse potencial de monetização, por sua vez, reflete, em princípio, a posição de gateway das empresas correspondentes. Ambos os indicadores também refletem a capacidade financeira das empresas em questão, incluindo sua capacidade de aproveitar seu acesso aos mercados financeiros para fortalecer sua posição. Isso pode acontecer, por exemplo, quando esse acesso superior é usado para adquirir outras empresas, uma capacidade que, por sua vez, demonstrou ter potenciais efeitos negativos na inovação. A capitalização de mercado também pode refletir a posição futura esperada e o impacto das empresas em questão no mercado doméstico, mesmo que o faturamento atual possa ser relativamente baixo. O valor da capitalização de mercado deve basear-se num nível que reflita a capitalização de mercado média das maiores empresas cotadas num mercado regulamentado na União durante um período adequado.

(18) Embora uma capitalização de mercado igual ou superior ao limiar estabelecido no último ano financeiro deva dar Embora a presunção de que um provedor de serviços essenciais de plataforma tenha uma influência significativa no mercado interno não seja sustentada, uma capitalização de mercado sustentada do provedor de serviços essenciais de plataforma igual ou superior ao limite por três anos ou mais deve ser considerada para fortalecer ainda mais essa presunção.

- (19) Em vez disso, poderá haver uma série de factores relacionados com a capitalização de mercado que exigiriam uma avaliação aprofundada para determinar se uma empresa que fornece serviços essenciais de plataforma deve ser considerada como tendo uma influência significativa no mercado interno. Esse pode ser o caso em que a capitalização de mercado do provedor de serviços principais da plataforma em anos anteriores estava bem abaixo do limite e a volatilidade de sua capitalização de mercado ao longo do período observado era desproporcional à volatilidade geral do mercado de ações ou a trajetória de sua capitalização de mercado em comparação com as tendências de mercado era inconsistente com o crescimento rápido e unidirecional.
- (20) Ter um número muito elevado de utilizadores empresariais que dependem de um serviço de plataforma central para atingir um número muito elevado de utilizadores finais activos mensais permite à empresa que fornece esse serviço influenciar as operações de uma grande proporção de utilizadores empresariais a seu favor e indica, em princípio, que essa empresa constitui uma porta de entrada importante. Os respetivos níveis relevantes para esses valores devem ser definidos de modo a representarem uma percentagem substancial de toda a população da União, no que diz respeito aos utilizadores finais, e de toda a população de empresas que utilizam serviços essenciais de plataforma, a fim de determinar o limiar para os utilizadores empresariais. Usuários finais activos e usuários comerciais devem ser identificados e calculados para representar adequadamente a função e o escopo do serviço principal da plataforma específica em questão. A fim de proporcionar segurança jurídica aos controladores de acesso, os elementos para determinar o número de utilizadores finais activos e de utilizadores profissionais por serviço básico de plataforma devem ser estabelecidos no anexo do presente regulamento. Esses elementos podem ser afetados por desenvolvimentos técnicos e de outra natureza. A Comissão deverá, por conseguinte, ter poderes para adotar atos delegados para alterar o presente regulamento, atualizando a metodologia e a lista de indicadores utilizados para determinar o número de utilizadores finais activos e de utilizadores empresariais activos.
- (21) A empresa que fornece o serviço de plataforma principal goza de uma posição forte e duradoura nas suas operações ou é provável que venha a gozar de tal posição no futuro, em especial quando a contestabilidade da sua posição é limitada. É provável que isso aconteça quando a empresa tiver fornecido um serviço de plataforma essencial em pelo menos três Estados-Membros a um grande número de utilizadores empresariais e finais durante um período de pelo menos três anos.
- (22) Estes limiares podem ser afetados pela evolução do mercado e pelos desenvolvimentos técnicos. A Comissão deverá, portanto, ter poderes para adotar atos delegados a fim de especificar a metodologia para determinar se os limiares quantitativos são cumpridos e ajustá-la periodicamente à evolução do mercado e aos desenvolvimentos técnicos, sempre que necessário. Esses atos delegados não devem modificar os limiares quantitativos estabelecidos no presente regulamento.
- (23) Uma empresa que presta serviços essenciais de plataforma deverá poder refutar, em circunstâncias excepcionais, a presunção de que a empresa tem uma influência significativa no mercado interno, demonstrando que, embora cumpra os limiares quantitativos estabelecidos no presente regulamento, não cumpre os requisitos para ser designada como controlador de acesso. O ónus da prova de que a presunção decorrente do facto de os limiares quantitativos terem sido atingidos não se aplica deve recair sobre essa empresa. Na sua avaliação das provas e argumentos apresentados, a Comissão deverá apenas ter em conta os elementos que estejam diretamente relacionados com os critérios quantitativos, em especial a influência da empresa que fornece serviços essenciais de plataforma no mercado interno para além das receitas ou da capitalização bolsista, como a sua dimensão em termos absolutos e o número de Estados-Membros em que está presente; em que medida o número real de usuários empresariais e usuários finais excede os limites e a importância do serviço de plataforma principal da empresa, levando em consideração a escala geral das atividades do serviço de plataforma principal em questão; e o número de anos em que os limites foram atingidos.

Qualquer justificativa econômica destinada a definir o mercado ou demonstrar eficiências decorrentes de um tipo específico de comportamento da empresa que fornece serviços básicos de plataforma deve ser descartada, pois não é relevante para a designação como gatekeeper. Se os argumentos apresentados não forem suficientemente fundamentados porque não colocam manifestamente em causa a presunção, a Comissão deverá poder rejeitar os argumentos no prazo de 45 dias úteis previsto para a designação. A Comissão deve poder tomar uma decisão com base nas informações disponíveis sobre os limites quantitativos no caso de uma empresa que fornece serviços essenciais de plataforma obstruir a investigação ao violar as medidas de investigação adotadas pela Comissão.

- (24) Deverá também ser prevista uma avaliação do papel de guardião das empresas que prestam serviços essenciais de plataforma que não cumprem todos os limiares quantitativos, à luz dos requisitos objetivos gerais de que têm uma influência significativa no mercado interno, funcionam como uma importante porta de entrada para os utilizadores empresariais chegarem aos utilizadores finais e desfrutam ou são suscetíveis de alcançar uma posição forte e duradoura nas suas operações num futuro próximo. Quando a empresa que fornece serviços essenciais de plataforma for uma pequena, média ou microempresa, a avaliação deverá considerar cuidadosamente se tal empresa poderá prejudicar substancialmente a disputabilidade dos serviços essenciais de plataforma, dado que o presente regulamento se dirige principalmente a grandes empresas com poder económico considerável, e não a pequenas, médias ou microempresas.
- (25) Tal avaliação só pode ser efectuada após uma investigação de mercado e tendo em conta limiares quantitativos. Em sua avaliação, a Comissão deve perseguir os objetivos de preservar e promover a inovação e a qualidade dos produtos e serviços digitais, a medida em que os preços são justos e competitivos e a medida em que a qualidade ou a escolha para usuários empresariais e usuários finais é ou permanece alta. Elementos específicos das empresas que fornecem os principais serviços de plataforma em questão podem ser levados em consideração, como economias extremas de escala ou escopo, efeitos de rede muito poderosos, benefícios de dados, capacidade de conectar muitos usuários comerciais a muitos usuários finais graças à natureza multilateral desses serviços, efeitos de bloqueio, falta de multiconexão, estrutura de conglomerado comercial ou integração vertical. Além disso, uma capitalização de mercado muito alta, uma relação património líquido/lucro muito alta ou um faturamento muito alto de usuários finais de um único serviço de plataforma principal podem ser usados como indicadores do potencial dessas empresas de influenciar e inclinar o mercado a seu favor. Juntamente com a capitalização de mercado, altas taxas de crescimento relativo são exemplos de parâmetros dinâmicos particularmente relevantes para identificar os principais provedores de serviços de plataforma que provavelmente se estabelecerão e perdurarão. A Comissão deve poder tomar uma decisão tirando conclusões adversas dos fatos disponíveis quando a empresa que fornece serviços essenciais de plataforma obstrui substancialmente a investigação ao não cumprir as medidas investigativas adotadas pela Comissão.
- (26) Deverá aplicar-se um subconjunto específico de regras às empresas que prestam serviços essenciais de plataforma e que se espera que gozem de uma posição forte e duradoura num futuro próximo. As características muito específicas dos principais serviços de plataforma os tornam propensos à inclinação do mercado a seu favor: uma vez que um provedor de serviços de plataforma principal tenha alcançado uma certa vantagem sobre seus rivais ou concorrentes potenciais em termos de tamanho ou poder de intermediação, sua posição pode se tornar inatacável e a situação pode evoluir a um ponto em que é provável que desfrute de uma posição forte e duradoura em um futuro próximo. As empresas podem tentar induzir esse viés de mercado e se estabelecer como guardiães recorrendo a algumas das condições e práticas injustas regulamentadas por este Regulamento. Em tal situação, parece apropriado intervir antes que ocorra uma inclinação irreversível do mercado.
- (27) No entanto, essa intervenção precoce deverá limitar-se à imposição apenas das obrigações que sejam necessárias e adequadas para garantir que os serviços em questão continuem a ser contestáveis e para evitar o risco qualificado de condições e práticas desleais. As obrigações que impedem o prestador de serviços de plataforma em questão de desfrutar de uma posição forte e duradoura nas suas operações, como as que impedem a alavancagem e as que facilitam a comutação e a multiconexão, estão mais diretamente orientadas para esse fim. Além disso, para garantir a proporcionalidade, a Comissão deverá aplicar desse subconjunto de obrigações apenas aquelas que forem necessárias e proporcionais para atingir os objetivos do presente regulamento e deverá rever periodicamente se essas obrigações devem ser mantidas, suprimidas ou adaptadas.
- (28) A aplicação apenas das obrigações que sejam necessárias e proporcionais à consecução dos objectivos do presente regulamento deverá permitir à Comissão intervir de forma atempada e eficaz, respeitando simultaneamente a proporcionalidade das medidas consideradas. Deve também tranquilizar os participantes do mercado, incluindo potenciais participantes, sobre a contestabilidade e a imparcialidade dos serviços relevantes.
- (29) Os controladores de acesso deverão cumprir as obrigações estabelecidas no presente regulamento relativamente a cada um dos serviços essenciais de plataforma enumerados na decisão de designação relevante. As obrigações devem ser aplicadas levando em consideração a posição do cluster dos gatekeepers, se aplicável. Além disso, a Comissão deverá poder impor medidas coercivas ao controlador de acesso através de uma

decisão. Essas medidas de implementação devem ser concebidas de forma eficaz, tendo em conta as características dos principais serviços de plataforma e os potenciais riscos de evasão, e de acordo com o princípio da proporcionalidade e os direitos fundamentais das empresas em causa, bem como os de terceiros.

- (30) A natureza tecnológica dos principais serviços de plataforma, que é complexa e evolui muito rapidamente, exige uma revisão periódica do estatuto dos guardiões, incluindo aqueles que se espera que alcancem uma posição forte e duradoura nas suas operações num futuro próximo. Para fornecer a todos os participantes do mercado, incluindo os gatekeepers, a certeza necessária em relação às obrigações legais aplicáveis, é necessário definir um prazo para essas revisões periódicas. Também é importante realizar essas revisões regularmente e pelo menos a cada três anos. Além disso, é importante esclarecer que nem toda mudança nos fatos com base nos quais um provedor de serviços básicos de plataforma foi nomeado como um gatekeeper deve exigir uma alteração na decisão de nomeação. A modificação só será necessária se a mudança nos fatos também resultar em uma alteração na avaliação. Para determinar se esse é o caso, é preciso fazer uma avaliação caso a caso dos fatos e circunstâncias.
- (31) A fim de salvaguardar a disputabilidade e a equidade dos serviços essenciais de plataforma prestados pelos controladores de acesso, deverá ser fornecido um conjunto de regras harmonizadas relativas a esses serviços de forma clara e inequívoca. Essas normas são necessárias para abordar o risco de efeitos nocivos das práticas de gatekeeper, em benefício do ambiente de negócios nos serviços relevantes, dos usuários e, em última análise, da sociedade como um todo. As obrigações se aplicam às práticas que são consideradas prejudiciais à contestabilidade ou injustas, ou ambas, ao levar em conta as características do setor digital e que têm um impacto direto particularmente negativo sobre os usuários empresariais e os usuários finais. Deverá ser possível que as obrigações estabelecidas no presente regulamento tenham especificamente em conta a natureza dos principais serviços de plataforma prestados. As obrigações previstas neste Regulamento não devem apenas garantir a contestabilidade e a imparcialidade em relação aos principais serviços de plataforma listados na decisão de designação, mas também em relação a outros produtos e serviços digitais em que os gatekeepers aproveitam sua posição de gateway, que geralmente são fornecidos ou prestados juntamente com ou em suporte aos principais serviços de plataforma.
- (32) Para efeitos do presente regulamento, a disputabilidade deverá referir-se à capacidade das empresas de ultrapassarem eficazmente as barreiras à entrada e à expansão e de competirem com o controlador de acesso com base na qualidade intrínseca dos seus produtos e serviços. As características dos principais serviços de plataforma no setor digital, como efeitos de rede, economias de escala significativas e benefícios baseados em dados, limitaram a contestabilidade desses serviços e ecossistemas relacionados. Essa baixa contestabilidade reduz os incentivos para inovar e melhorar produtos e serviços para o gatekeeper, seus usuários profissionais, seus concorrentes e clientes e, portanto, afeta negativamente o potencial de inovação da economia de plataforma online mais ampla. A contestabilidade de serviços no setor digital também pode ser limitada se houver mais de um guardião para um serviço de plataforma principal. O presente regulamento deverá, portanto, proibir determinadas práticas dos controladores de acesso que possam aumentar as barreiras à entrada ou à expansão e impor determinadas obrigações aos controladores de acesso que tendam a reduzir essas barreiras. As obrigações também devem abordar situações em que a posição do gatekeeper se tornou tão arraigada que a concorrência entre plataformas não é eficaz no curto prazo, o que implica que a concorrência intraplataforma ou o aumento da concorrência são necessários.
- (33) Para efeitos do presente regulamento, a injustiça deverá referir-se a um desequilíbrio entre os direitos e as obrigações dos utilizadores profissionais, em que o controlador de acesso obtém uma vantagem desproporcionada. Os participantes do mercado, incluindo usuários profissionais de serviços essenciais da plataforma e provedores alternativos de serviços fornecidos em conjunto com ou em suporte a tais serviços essenciais da plataforma, devem ser capazes de colher adequadamente os benefícios resultantes de seus esforços inovadores ou outros. Devido à sua posição de gateway e maior poder de barganha, os gatekeepers podem se envolver em comportamentos que não permitem que outros colham totalmente os benefícios de suas próprias contribuições e definir unilateralmente condições desequilibradas para o uso de seus principais serviços de plataforma ou serviços fornecidos em conjunto com ou em suporte aos seus principais serviços de plataforma. Este desequilíbrio não é excluído pelo facto de o gatekeeper oferecer um determinado serviço gratuitamente a um grupo específico de utilizadores, podendo também consistir na exclusão ou discriminação de utilizadores profissionais, nomeadamente se estes últimos concorrerem com os serviços prestados pelo gatekeeper. Este regulamento deve, portanto, impor obrigações aos controladores de acesso para abordarem esse tipo de comportamento.

- (34) A contestabilidade e a justiça estão inter-relacionadas. A falta de contestabilidade ou sua escassez em relação a um determinado serviço pode permitir que um gatekeeper se envolva em práticas desleais. Da mesma forma, Práticas desleais de um gatekeeper podem reduzir a capacidade de usuários profissionais ou terceiros de contestar a posição do gatekeeper. Portanto, uma obrigação específica ao abrigo deste Regulamento pode abordar ambos os elementos.
- (35) Consequentemente, as obrigações estabelecidas no presente regulamento são necessárias para dar resposta às preocupações de ordem pública identificadas, uma vez que não existem medidas alternativas menos restritivas que possam efetivamente alcançar o mesmo resultado, tendo em conta a necessidade de salvaguardar a ordem pública, proteger a privacidade e combater práticas comerciais fraudulentas e enganosas.
- (36) Os controladores de acesso recolhem frequentemente dados pessoais diretamente dos utilizadores finais com a finalidade de fornecer serviços de publicidade online quando os utilizadores finais utilizam sítios Web e aplicações informáticas de terceiros. Terceiros também fornecem aos gatekeepers dados pessoais de seus usuários finais para que eles possam utilizar determinados serviços fornecidos pelos gatekeepers no contexto de seus principais serviços de plataforma, como aqueles fornecidos a públicos personalizados. O processamento de dados pessoais de terceiros que usam serviços de plataforma essenciais com a finalidade de fornecer serviços de publicidade online oferece aos gatekeepers vantagens potenciais em termos de acumulação de dados, criando barreiras à entrada no mercado. Isso ocorre porque os controladores de dados processam dados pessoais de um número consideravelmente maior de terceiros do que outras empresas. Vantagens semelhantes surgem da prática de i) combinar dados pessoais de usuários finais coletados de um serviço de plataforma principal com dados coletados de outros serviços, ii) usar dados pessoais de um serviço de plataforma principal em outros serviços fornecidos separadamente pelo gatekeeper, em particular serviços que não são fornecidos em conjunto com ou em suporte ao serviço de plataforma principal relevante, e vice-versa, ou iii) registrar usuários finais em diferentes serviços de gatekeeper para combinar dados pessoais. Para garantir que os gatekeepers não comprometam injustamente a contestabilidade dos serviços principais da plataforma, eles devem permitir que os usuários finais escolham livremente se envolver em tais práticas de processamento de dados e login, oferecendo-lhes uma alternativa menos personalizada, mas equivalente, e sem condicionar o uso do serviço principal da plataforma ou certas funcionalidades dele ao consentimento do usuário final. Isto não deverá afetar o tratamento de dados pessoais nem o início de sessão dos utilizadores finais num serviço pelo controlador de acesso com base na base jurídica prevista no artigo 6.º, n.º 1, alíneas c), d) e e), do Regulamento (UE) 2016/679, mas não no artigo 6.º, n.º 1, alíneas b) e f), do mesmo regulamento.
- (37) A alternativa menos personalizada não deve ser diferente ou ter qualidade degradada em relação à alternativa serviço fornecido a usuários finais consentidos, a menos que a degradação na qualidade seja uma consequência direta da incapacidade do gatekeeper de processar tais dados pessoais e registrar usuários finais em um serviço. Não dar consentimento não deveria ser mais difícil do que dá-lo. Quando o gatekeeper solicita consentimento, ele deve apresentar proativamente ao usuário final uma solução fácil de usar para fornecer, modificar ou retirar o consentimento de maneira expressa, clara e simples. Em particular, o consentimento deve ser dado por meio de uma ação afirmativa ou declaração clara que estabeleça uma manifestação de acordo livre, específico, informado e inequívoco por parte do usuário final, conforme definido no Regulamento (UE) 2016/679. No momento do consentimento, e somente quando aplicável, o usuário final deve ser informado de que a não autorização pode resultar em uma oferta menos personalizada, mas que, caso contrário, o serviço principal da plataforma permanecerá inalterado e nenhuma funcionalidade será removida. Excepcionalmente, se o consentimento não puder ser fornecido diretamente ao serviço de plataforma principal do gatekeeper, os usuários finais deverão ser capazes de fornecer consentimento por meio de cada serviço de terceiros que faça uso desse serviço de plataforma principal, para que o gatekeeper processe dados pessoais com a finalidade de fornecer serviços de publicidade online.

Por fim, deve ser tão fácil retirar o consentimento quanto concedê-lo. Os gatekeepers não devem projetar, organizar ou operar suas interfaces on-line de maneira que engane ou manipule os usuários finais ou que de outra forma reduza ou distorça materialmente sua capacidade de dar consentimento livremente. Em particular, os controladores não devem ser autorizados a solicitar aos usuários finais mais de uma vez por ano que forneçam consentimento para a mesma finalidade de processamento para a qual inicialmente não forneceram consentimento ou retiraram o consentimento. O presente regulamento não prejudica o Regulamento (UE) 2016/679, incluindo o seu quadro de execução, que continua a ser plenamente aplicável a qualquer reclamação dos titulares dos dados relativa a uma violação dos seus direitos ao abrigo desse regulamento.

- (38) Os menores merecem protecção específica no que diz respeito aos seus dados pessoais, em especial no que diz respeito à utilização dos seus dados pessoais para fins de comunicação comercial ou à criação de perfis de utilizador. A protecção de menores online é um objetivo importante da União e deve ser refletida na sua legislação aplicável. Neste contexto, deve ser tida em conta uma regulamentação sobre um mercado único para serviços digitais. Nada no presente regulamento isenta os controladores de acesso da obrigação de proteger as crianças ao abrigo da legislação aplicável da União.
- (39) Em certos casos, por exemplo, através da imposição de condições contratuais, os controladores podem restringir a capacidade dos utilizadores profissionais dos seus serviços de intermediação em linha de oferecerem produtos ou serviços aos utilizadores finais em condições mais favoráveis, incluindo o preço, através de outros serviços de intermediação em linha ou dos seus canais de venda directos em linha. Quando tais restrições se referem para serviços de intermediação on-line de terceiros, limitam a contestabilidade entre plataformas, o que, por sua vez, limita as opções de serviços alternativos de intermediação on-line para usuários finais. Quando tais restrições se referem a canais de vendas directas on-line, elas limitam injustamente a liberdade dos usuários profissionais de usar tais canais. Para garantir que os usuários profissionais de serviços de intermediação on-line de gatekeepers sejam livres para escolher serviços alternativos de intermediação on-line ou canais de vendas on-line directos e para diferenciar as condições sob as quais oferecem seus produtos ou serviços aos usuários finais, não deve ser aceitável que os gatekeepers limitem a possibilidade de usuários profissionais escolherem diferenciar as condições comerciais, incluindo o preço. Essa restrição deve ser aplicada a qualquer medida com efeito equivalente, como aumentar as taxas de comissão ou remover ofertas de usuários profissionais.
- (40) A fim de evitar aumentar ainda mais a sua dependência dos serviços essenciais de plataforma fornecidos pelos controladores de acesso e de promover a multiconexão, os utilizadores empresariais desses controladores de acesso deverão ser livres de promover e escolher o canal de distribuição que considerem mais adequado para interagir com quaisquer utilizadores finais que esses utilizadores empresariais já tenham adquirido através dos serviços essenciais de plataforma fornecidos pelo controlador de acesso ou através de outros canais. Isto se aplica à promoção de ofertas, também por meio de um aplicativo de computador do usuário profissional, e a qualquer forma de comunicação e celebração de contratos entre usuários profissionais e usuários finais. Um Usuário Final é considerado um Usuário Final Adquirido se já tiver estabelecido um relacionamento comercial com o Usuário Empresarial e, quando aplicável, o Gatekeeper tiver sido compensado direta ou indiretamente pelo Usuário Empresarial por facilitar a aquisição inicial do Usuário Final pelo Usuário Empresarial. Essas relações comerciais podem envolver uma taxa ou ser gratuitas (como testes gratuitos ou níveis de serviço gratuitos) e podem ter sido estabelecidas no serviço de plataforma principal do Gatekeeper ou por meio de qualquer outro canal. Além disso, os usuários finais também devem ser livres para escolher ofertas desses usuários profissionais e celebrar contratos com eles por meio dos serviços de plataforma principais do gatekeeper, quando aplicável, ou por meio de um canal de distribuição direto do usuário profissional ou outro canal indireto usado por esse usuário profissional.
- (41) A capacidade dos utilizadores finais de adquirirem conteúdos, assinaturas, benefícios ou outros itens fora dos serviços de plataforma principais dos controladores de acesso não deverá ser prejudicada ou restringida. Em particular, deve-se evitar uma situação em que os gatekeepers restrinjam os usuários finais de acessar e usar tais serviços por meio de um aplicativo de computador executado em seu serviço de plataforma principal. Por exemplo, assinantes de conteúdo online adquirido fora de um aplicativo de computador, loja de aplicativos ou assistente virtual não devem ser impedidos de acessar tal conteúdo online por meio de um aplicativo de computador executado no serviço de plataforma principal do gatekeeper simplesmente porque o conteúdo foi adquirido fora de tal aplicativo, loja de aplicativos ou assistente virtual.
- (42) A fim de salvaguardar um ambiente de negociação justo e proteger a disputabilidade do setor digital, é importante salvaguardar o direito dos utilizadores empresariais e dos utilizadores finais, incluindo os denunciantes, de expressarem as suas preocupações a qualquer autoridade administrativa ou pública relevante, incluindo os tribunais nacionais, sobre práticas desleais dos controladores de acesso que levam a uma questão de incumprimento da legislação aplicável da União ou nacional. Por exemplo, os utilizadores empresariais ou os utilizadores finais podem querer reclamar sobre diferentes tipos de práticas desleais, como condições de acesso discriminatórias, encerramento injustificado de contas de utilizadores empresariais ou razões pouco claras para tal.

descontinuar produtos. Qualquer prática que impeça ou dificulte de alguma forma que esses usuários expressem suas preocupações ou solicitem indenização, por exemplo, por meio de cláusulas de confidencialidade em acordos ou outras condições estabelecidas por escrito, deve, portanto, ser proibida. Esta proibição não prejudica o direito dos utilizadores empresariais e dos guardiões de definir os termos de utilização nos seus acordos, incluindo o recurso a mecanismos legais para o tratamento de reclamações e qualquer recurso a mecanismos alternativos de resolução de litígios ou à jurisdição de tribunais especiais, em conformidade com a legislação da União e nacional. Isso deve ser entendido sem prejuízo do papel desempenhado pelos gatekeepers no combate ao conteúdo ilegal online.

- (43) Alguns dos serviços prestados em conjunto com ou em apoio aos serviços de plataforma essenciais relevantes do controlador de acesso, tais como serviços de identificação, motores de navegação na Web, serviços de pagamento ou serviços técnicos de apoio à prestação de serviços de pagamento, tais como sistemas de pagamento para compras em aplicações, são cruciais para que os utilizadores empresariais possam exercer a sua atividade profissional e otimizar os seus serviços. Por exemplo, todos os navegadores da web são baseados em um mecanismo de navegador da web, do qual dependem elementos essenciais da funcionalidade do navegador, como velocidade, confiabilidade e compatibilidade com a web. Quando os gatekeepers gerenciam e aplicam mecanismos de navegadores da web, eles estão em posição de determinar a funcionalidade e os padrões aplicáveis não apenas aos seus próprios navegadores, mas também aos navegadores concorrentes e, por sua vez, aos aplicativos da web. Por esse motivo, os gatekeepers não devem usar sua posição para exigir que seus usuários comerciais dependentes usem quaisquer serviços fornecidos em conjunto com, ou em suporte aos, serviços principais da plataforma pelos próprios gatekeepers como parte da prestação de serviços ou fornecimento de produtos por esses usuários comerciais. Para evitar uma situação em que os gatekeepers imponham indiretamente aos usuários empresariais seus próprios serviços fornecidos em conjunto com, ou em suporte a, serviços de plataforma principais, os gatekeepers devem ainda ser proibidos de exigir que os usuários finais utilizem tais serviços, quando tal exigência for imposta no contexto do serviço fornecido aos usuários finais pelo usuário empresarial que utiliza o serviço de plataforma principal do gatekeeper. O objetivo desta proibição é proteger a liberdade do usuário profissional de escolher serviços alternativos aos fornecidos pelo gatekeeper, embora não deva ser interpretada como uma obrigação do usuário profissional de oferecer tais alternativas aos seus usuários finais.
- (44) Exigir que os utilizadores empresariais ou os utilizadores finais subscrevam ou se registem em qualquer outro serviço de plataforma essencial do controlador de acesso listado na decisão de designação ou que atinjam os limites para utilizadores finais ativos e utilizadores empresariais definidos no presente regulamento, como condição para utilizar, aceder ou registar-se num serviço de plataforma essencial, fornece aos controladores de acesso um meio para atrair e reter novos utilizadores empresariais e utilizadores finais para os seus serviços de plataforma essenciais, garantindo que os utilizadores empresariais não podem aceder a um serviço de plataforma essencial sem, pelo menos, se registarem ou criarem uma conta para receberem um segundo serviço de plataforma essencial. Esse comportamento também oferece aos gatekeepers uma vantagem potencial em termos de acúmulo de dados. Dessa forma, tal conduta pode criar barreiras à entrada no mercado e deve ser proibida.
- (45) As condições em que os controladores de acesso fornecem serviços de publicidade online aos utilizadores empresariais, incluindo anunciantes e editores, são frequentemente pouco transparentes e opacas. Essa opacidade está em parte ligada às práticas de algumas plataformas, mas também se deve à grande complexidade da publicidade programática hoje. O setor parece ter se tornado menos transparente após a introdução de uma nova legislação de privacidade. Isso geralmente leva à falta de informação e conscientização por parte de anunciantes e editores sobre os termos e condições dos serviços de publicidade online que eles compram e prejudica sua capacidade de mudar de provedor de serviços de publicidade online. Além disso, os custos dos serviços de publicidade online nessas condições provavelmente serão mais altos do que seriam em um ambiente de plataforma mais equitativo, transparente e contestável. Esses custos mais altos provavelmente se refletem nos preços que os usuários finais pagam por muitos produtos e serviços cotidianos que dependem do uso de serviços de publicidade online. As obrigações de transparência devem, portanto, exigir que os guardiões, mediante solicitação, forneçam aos anunciantes e editores aos quais prestam serviços de publicidade online informações gratuitas que permitam que ambas as partes entendam o preço pago por cada um dos diferentes serviços de publicidade online fornecidos dentro da cadeia de valor de publicidade relevante.

Essas informações devem ser fornecidas ao anunciante, mediante solicitação, para cada anúncio, em relação ao preço e às comissões cobradas a esse anunciante e, com o consentimento do editor que possui o inventário no qual o anúncio aparece, a remuneração recebida por esse editor consentente. O fornecimento diário dessas informações permitirá que os anunciantes recebam informações com um nível de detalhes suficiente para comparar o custo de uso dos serviços de publicidade online dos gatekeepers com o custo de uso dos serviços de publicidade online de outras empresas. Caso alguns editores não consigam no fornecimento de informações relevantes ao anunciante, o gatekeeper deve fornecer ao anunciante as

informações do anunciante sobre a remuneração média diária recebida pelos referidos editores pelos anúncios correspondentes. As mesmas obrigações e princípios para fornecer informações relevantes relacionadas ao fornecimento de serviços de publicidade on-line devem ser aplicados às solicitações dos editores. Como os gatekeepers podem usar diferentes modelos de preços para fornecer serviços de publicidade online a anunciantes e editores – por exemplo, eles podem definir um preço por impressão ou por visualização, ou com base em qualquer outro critério – os gatekeepers também devem fornecer o método pelo qual cada um dos preços e remunerações são calculados.

- (46) Em determinadas circunstâncias, o guardião desempenha um duplo papel: por um lado, é um fornecedor de serviços de plataforma essenciais que fornece aos seus utilizadores empresariais um serviço de plataforma essencial e, possivelmente, outros serviços prestados em conjunto com os serviços de plataforma essenciais ou em apoio a eles; Por outro lado, compete ou tenta competir com esses mesmos usuários profissionais no fornecimento ou fornecimento aos mesmos usuários finais de serviços ou produtos idênticos ou semelhantes. Nessas circunstâncias, um gatekeeper pode tirar proveito de sua dupla função para usar dados gerados ou fornecidos por seus usuários comerciais em conexão com as atividades de tais usuários comerciais ao usar os serviços principais da plataforma, ou serviços fornecidos em conjunto com ou em suporte aos serviços principais da plataforma, para o benefício de seus próprios serviços ou produtos. Os Dados do Usuário Comercial também podem incluir dados gerados ou fornecidos durante suas atividades de usuário final. Este pode ser o caso, por exemplo, quando um gatekeeper oferece um mercado online ou uma loja de aplicativos para usuários empresariais e, ao mesmo tempo, fornece serviços como um varejista online ou provedor de serviços de aplicativos. Para evitar que os gatekeepers se beneficiem injustamente de sua dupla função, é necessário garantir que eles não usem dados agregados ou desagregados de qualquer tipo, o que pode incluir dados pessoais e anônimos não públicos, para fornecer serviços semelhantes aos seus usuários comerciais. Essa obrigação deve se aplicar ao gatekeeper como um todo, incluindo, mas não se limitando, à sua unidade de negócios que compete com os usuários profissionais de um serviço básico de plataforma.
- (47) Os utilizadores empresariais também podem contratar serviços de publicidade online de um fornecedor de serviços de plataforma central para fornecer produtos e prestar serviços aos utilizadores finais. Nesse caso, pode acontecer que os dados não sejam gerados no serviço principal da plataforma, mas sejam fornecidos ao serviço principal da plataforma pelo usuário profissional ou gerados a partir de suas operações por meio do serviço principal da plataforma correspondente. Em alguns casos, o serviço de plataforma principal que fornece publicidade pode ter uma função dupla: como provedor de serviços de publicidade on-line e como provedor de serviços que competem com aqueles de seus usuários empresariais. A obrigação que proíbe um guardião de dupla função de usar dados de usuários empresariais deve, portanto, aplicar-se também em relação aos dados que um serviço de plataforma principal recebeu de empresas com a finalidade de fornecer serviços de publicidade on-line relacionados a esse serviço de plataforma principal.
- (48) No que diz respeito aos serviços de computação em nuvem, a obrigação de não utilizar dados de utilizadores empresariais deverá estender-se aos dados fornecidos ou gerados pelos utilizadores empresariais do controlador de acesso quando utilizam o serviço de computação em nuvem do controlador de acesso, ou através da sua loja de aplicações informáticas que permite aos utilizadores finais dos serviços de computação em nuvem aceder às aplicações informáticas. Essa obrigação não deve afetar o direito do controlador de acesso de usar dados agregados para a prestação de outros serviços prestados em conjunto com ou em suporte aos seus principais serviços de plataforma, como serviços de análise de dados, desde que as disposições do Regulamento (UE) 2016/679 e da Diretiva 2002/58/CE sejam cumpridas e as obrigações relevantes deste regulamento relativas a tais serviços sejam respeitadas.
- (49) Um gatekeeper pode utilizar diferentes meios para favorecer os seus próprios serviços ou produtos ou os de terceiros no seu sistema operativo, assistente virtual ou navegador web, em detrimento dos mesmos serviços ou de serviços semelhantes que os utilizadores finais poderiam obter através de outros terceiros. Isso pode ocorrer, por exemplo, quando os controladores de acesso pré-instalam determinados aplicativos ou serviços de computador. Para oferecer opções ao usuário final, os gatekeepers não devem impedir que os usuários finais desinstalem qualquer aplicativo de software de seu sistema operacional. Os gatekeepers devem ser capazes de restringir tal desinstalação somente quando os aplicativos em questão forem essenciais para a operação do sistema operacional ou dispositivo. Da mesma forma, os controladores de acesso devem permitir que os utilizadores finais alterem facilmente as definições predefinidas do sistema operativo, do assistente virtual ou do navegador da Web quando

Essa configuração padrão favorece seus próprios aplicativos e serviços de computador. Para fazer isso, eles podem, por exemplo, fazer com que uma tela de escolha apareça no momento em que o usuário usa pela primeira vez um mecanismo de busca on-line, assistente virtual ou navegador da web do gatekeeper listado na decisão de designação, permitindo que os usuários finais selecionem um serviço padrão alternativo quando o sistema operacional do gatekeeper direciona os usuários finais para o mecanismo de busca, assistente virtual ou navegador da web listado, ou quando o assistente virtual ou navegador da web do gatekeeper direciona o usuário para o mecanismo de busca on-line listado na decisão de designação.

- (50) As regras que um controlador estabelece para a distribuição de aplicações informáticas podem, em determinadas circunstâncias, restringir a capacidade dos utilizadores finais de instalarem e utilizarem eficazmente aplicações informáticas de terceiros ou lojas de aplicações informáticas nos sistemas operativos de computador ou lojas de aplicativos de computador fora dos serviços de plataforma principais desse gatekeeper. Essas restrições podem limitar a capacidade dos desenvolvedores de aplicativos de software de usar canais de distribuição alternativos e a capacidade dos usuários finais de escolher entre diferentes aplicativos de software de diferentes canais de distribuição e devem ser proibidas, pois são injustas e podem prejudicar a contestabilidade dos principais serviços da plataforma. Para garantir a contestabilidade, o gatekeeper também deve permitir que aplicativos de software de terceiros ou lojas de aplicativos solicitem ao usuário final que decida se tal serviço deve se tornar o serviço padrão e permitir que a alteração seja feita facilmente.

Para garantir que aplicativos de software de terceiros ou lojas de aplicativos de software não comprometam a integridade do sistema operacional fornecido pelo controlador de acesso, o controlador de acesso em causa deverá poder aplicar medidas técnicas ou contratuais proporcionais para esse efeito, se demonstrar que tais medidas são necessárias e justificadas e que não existem meios menos restritivos para salvaguardar a integridade do sistema operacional. A integridade do sistema operacional deve incluir todas as opções de design que precisam ser aplicadas e mantidas para que o sistema operacional seja protegido contra acesso não autorizado, garantindo que os controles de segurança especificados para o sistema operacional em questão. Além disso, para garantir que aplicativos de computador de terceiros ou lojas de aplicativos de computador não comprometam a segurança dos usuários finais, o gatekeeper deve ser capaz de aplicar medidas e ajustes estritamente necessários e proporcionais que não façam parte da configuração padrão e que permitam aos usuários finais proteger efetivamente a segurança em relação a aplicativos de computador de terceiros ou lojas de aplicativos de computador, desde que o gatekeeper demonstre que tais medidas e ajustes são estritamente necessários e justificadas e que não há alternativas menos restritivas para atingir esse objetivo. O gatekeeper deve ser impedido de incluir tais medidas na configuração padrão ou pré-instalá-las.

- (51) Os gatekeepers estão frequentemente integrados verticalmente e oferecem determinados produtos ou serviços aos utilizadores finais através dos seus próprios serviços de plataforma principais, ou através de um utilizador profissional sobre o qual exercem controlo, o que frequentemente conduz a conflitos de interesses. Esse é o caso quando um gatekeeper fornece seus próprios serviços de intermediação online por meio de um mecanismo de busca online. Ao oferecer tais produtos ou serviços no serviço de plataforma principal, os gatekeepers podem reservar uma posição melhor para sua própria oferta, em termos de classificação e funções de indexação e rastreamento relacionadas, do que para produtos ou serviços de terceiros que também operam naquele serviço de plataforma principal. Isso pode ocorrer, por exemplo, com produtos ou serviços, incluindo outros serviços essenciais da plataforma, que são classificados nos resultados de mecanismos de busca on-line ou que são parcial ou totalmente integrados aos resultados de mecanismos de busca on-line, grupos de resultados especializados em um determinado tópico, exibidos junto com os resultados de um mecanismo de busca on-line, que são considerados ou usados por certos usuários finais como um serviço distinto ou adicional ao mecanismo de busca on-line.

Outros exemplos incluem aplicativos de computador distribuídos por meio de lojas de aplicativos de computador, vídeos distribuídos por meio de plataformas de compartilhamento de vídeos, produtos ou serviços destacados e exibidos na seção de notícias de um serviço de rede social on-line, produtos ou serviços classificados em resultados de pesquisa ou exibidos em um mercado on-line ou produtos ou serviços oferecidos por meio de um assistente virtual. Os gatekeepers podem reservar uma posição melhor para sua própria oferta antes mesmo da classificação após uma pesquisa, por exemplo, durante o rastreamento e a indexação. Assim, os guardiões do acesso

Eles podem favorecer seu próprio conteúdo em detrimento do de terceiros já na fase de rastreamento, que é o processo de descoberta de conteúdo novo e atualizado, e durante a indexação, que envolve armazenar e organizar o conteúdo encontrado durante o processo de rastreamento. Nesses casos, os gatekeepers têm uma função dupla: intermediários para empresas terceirizadas e para empresas que fornecem ou prestam serviços diretamente. Consequentemente, esses guardiões têm a capacidade de minar diretamente a contestabilidade dos produtos ou serviços oferecidos nesses serviços de plataforma principais, em detrimento dos usuários profissionais que não são controlados pelos guardiões.

- (52) Nessas situações, os controladores de acesso não devem conceder qualquer tratamento diferenciado ou preferencial, no que diz respeito à classificação no serviço de plataforma principal e às funções de indexação e de rastreio relacionadas, seja através de meios legais, comerciais ou técnicos, a produtos ou serviços que oferecem diretamente ou através de utilizadores profissionais sob o seu controlo. Para garantir que esta obrigação seja efetiva, as condições aplicáveis à tal classificação também devem ser, em geral, justas e transparentes. Nesse sentido, a classificação deve abranger todas as formas de destaque relativo, incluindo exibição, classificação, geração de links ou resultados de voz, e também deve incluir casos em que um serviço de plataforma principal apresenta ou comunica ao usuário final apenas um resultado. Para garantir que esta obrigação seja eficaz e não possa ser contornada, ela também deve ser aplicada a qualquer medida que tenha um efeito equivalente ao do tratamento diferenciado ou preferencial na classificação. As orientações adotadas nos termos do artigo 5.º do Regulamento (UE) 2019/1150 deverão também facilitar a implementação e a execução desta obrigação.
- (53) Os controladores de acesso não devem restringir ou impedir a livre escolha dos utilizadores finais, impedindo-os, técnica ou de outra forma, de alternar entre aplicações e serviços informáticos ou de subscrever diferentes aplicações e serviços informáticos. Isso permite que mais empresas ofereçam seus serviços, proporcionando aos usuários finais uma maior variedade de opções. Os guardiões devem garantir a livre escolha, independentemente de serem ou não os fabricantes de qualquer ferragem através dos quais tais aplicações ou serviços informáticos são acedidos e não devem criar obstáculos artificiais, técnicos ou de outro tipo, que tornem impossível ou ineficaz a sua alteração. A mera oferta de um determinado produto ou serviço aos consumidores, inclusive por meio de pré-instalação, bem como a melhoria do que é oferecido aos usuários finais, como descontos de preço ou maior qualidade, não devem ser interpretados como um obstáculo proibido à mudança.
- (54) Os controladores de acesso podem prejudicar a capacidade dos utilizadores finais de aceder a conteúdos e serviços online, incluindo aplicações informáticas. Portanto, regras devem ser estabelecidas para garantir que a conduta dos gatekeepers não comprometa o direito dos usuários finais de acessar uma Internet aberta. Os guardiões também podem limitar tecnicamente a capacidade dos utilizadores finais de mudarem efectivamente de um fornecedor de serviços de Internet para outro, em particular através do controlo que exercem sobre ferragens ou sistemas operacionais. Isso distorce a igualdade de condições para os serviços de acesso à Internet e, em última análise, prejudica os usuários finais. Portanto, é necessário garantir que os controladores não imponham restrições indevidas aos usuários finais no que diz respeito à escolha do provedor de serviços de acesso à Internet.
- (55) Os gatekeepers podem fornecer serviços ou fornecer ferragens, como dispositivos portáteis, que acessam as funções de ferragens ou o Programa de um dispositivo que é acessado ou controlado por meio de um sistema operacional ou assistente virtual para fornecer funcionalidades específicas aos usuários finais. Nesse caso, para poder oferecer uma oferta competitiva aos utilizadores finais, prestadores de serviços ou fornecedores de ferragens Concorrentes, como fornecedores de dispositivos portáteis, precisam de interoperabilidade igualmente eficaz com a mesma funcionalidade de ferragens ou de software, e acesso a tais funções para fins de interoperabilidade.
- (56) Os gatekeepers também podem ter um papel duplo como desenvolvedores de sistemas operacionais e fabricantes de dispositivos, em particular de qualquer funcionalidade técnica que esses dispositivos possam ter. Por exemplo, um gatekeeper que é fabricante de um dispositivo pode restringir o acesso a algumas das funcionalidades desse dispositivo, como os elementos de segurança e processadores seguros da tecnologia de comunicação de campo próximo, mecanismos de autenticação e Programa usado para operar tais tecnologias, que podem ser necessárias para tornar eficaz o fornecimento de um serviço fornecido em conjunto com ou em suporte a um serviço de plataforma principal pelo gatekeeper ou qualquer empresa terceirizada que forneça tal serviço.

- (57) Se essa dualidade de funções for utilizada de modo a impedir outros prestadores de serviços ou fornecedores de ferragens acesso, em igualdade de condições, às mesmas funções do sistema operativo, ferragens ou do Programasque pode ser acessado ou usado pelo gatekeeper ao fornecer seus próprios serviços ou fornecer seus próprios ferragens complementares ou de suporte, a capacidade de inovação desses outros provedores ou fornecedores pode ser consideravelmente prejudicada, bem como a variedade de opções para os usuários finais. Por conseguinte, os gatekeepers devem ser obrigados a garantir, gratuitamente, uma interoperabilidade eficaz com as mesmas funções do sistema operativo, ferragens ou do Programasque pode ser acessado ou usado pelo gatekeeper ao fornecer seus próprios serviços ou fornecer seus próprios ferragens funções complementares e de suporte, bem como acesso a tais funções para fins de interoperabilidade. Esse acesso também pode ser exigido por aplicativos de computador relacionados aos serviços relevantes fornecidos em conjunto com, ou em suporte aos, serviços principais da plataforma, a fim de desenvolver e fornecer efetivamente funcionalidades que sejam interoperáveis com aquelas oferecidas pelos gatekeepers. O objetivo desta obrigação é permitir que empresas concorrentes se conectem por meio de interfaces ou soluções semelhantes às funções correspondentes com a mesma eficiência dos serviços ou do ferragens do porteiro.
- (58) As condições em que os controladores de acesso fornecem serviços de publicidade online aos utilizadores empresariais, incluindo anunciantes e editores, são frequentemente pouco transparentes e opacas. Isso geralmente leva à falta de informação para anunciantes e editores sobre o efeito de um determinado anúncio. Para aumentar ainda mais a imparcialidade, a transparência e a contestabilidade dos serviços de publicidade on-line listados na decisão de designação, bem como aqueles totalmente integrados a outros serviços de plataforma principais da mesma empresa, os gatekeepers devem, mediante solicitação, fornecer aos anunciantes e editores, e a terceiros autorizados por anunciantes e editores, acesso gratuito às ferramentas de medição de desempenho dos gatekeepers e aos dados — incluindo dados agregados e desagregados — necessários para permitir que anunciantes, terceiros autorizados, como agências de publicidade agindo em nome de uma empresa de publicidade, e editores realizem sua própria verificação independente do fornecimento dos serviços de publicidade on-line relevantes.
- (59) Os guardiões beneficiam do acesso a grandes quantidades de dados que recolhem quando prestam serviços de plataforma essenciais, bem como outros serviços digitais. Para garantir que os gatekeepers não comprometam a contestabilidade dos principais serviços da plataforma ou o potencial de inovação de um setor digital dinâmico ao impor restrições à troca de serviços ou à multiconexão, os usuários finais, bem como terceiros autorizados por um usuário final, devem ter acesso efetivo e imediato aos dados que forneceram ou geraram por meio de sua atividade nos principais serviços da plataforma do gatekeeper. Os dados devem ser recebidos em um formato que permita ao usuário final ou ao terceiro relevante autorizado pelo usuário final que recebe os dados acessá-los e utilizá-los de forma imediata e eficaz. Os gatekeepers também devem garantir, por meio de medidas técnicas adequadas e de qualidade, como interfaces de programação de aplicativos, que os usuários finais ou terceiros autorizados pelos usuários finais possam transferir dados livremente, de forma contínua e em tempo real. Isso também deve se aplicar a todos os outros dados em diferentes níveis de agregação que são necessários para permitir efetivamente essa portabilidade. Por uma questão de clareza, a obrigação do controlador de acesso de garantir a portabilidade efetiva dos dados ao abrigo do presente regulamento é complementar ao direito à portabilidade dos dados estabelecido no Regulamento (UE) 2016/679. Facilitar a comutação ou a multiconexão deve, por sua vez, levar a uma maior escolha para os usuários finais e servir como um incentivo para que os gatekeepers e usuários profissionais inovem.
- (60) Os utilizadores profissionais que utilizam serviços de plataforma essenciais fornecidos por gatekeepers e os utilizadores finais desses utilizadores profissionais fornecem e geram uma grande quantidade de dados. Para garantir que os usuários empresariais tenham acesso aos dados relevantes gerados dessa maneira, os gatekeepers devem, mediante solicitação, fornecer acesso efetivo e gratuito a esses dados. Este acesso também deve ser concedido a terceiros contratados por usuários profissionais que atuam como processadores de dados para usuários profissionais. O acesso incluirá o acesso aos dados fornecidos ou gerados pelos mesmos usuários comerciais e pelos mesmos usuários finais desses usuários comerciais no contexto de outros serviços fornecidos pelo mesmo gatekeeper, incluindo serviços fornecidos em conjunto com ou em suporte aos principais serviços da plataforma, se estiverem inextricavelmente vinculados à solicitação relevante. Para esse fim, os guardiões não devem usar quaisquer restrições contratuais ou de outra natureza para impedir que os usuários empresariais acessem os dados relevantes e devem permitir que os usuários empresariais obtenham o consentimento de seus usuários finais para acessar e obter os dados, quando tal consentimento for exigido pelo Regulamento (UE) 2016/679 e pela Diretiva 2002/58/CE. Os gatekeepers também devem garantir acesso contínuo e em tempo real a esses dados por meio de medidas técnicas apropriadas, por exemplo, interfaces de programação de aplicativos de alta qualidade ou ferramentas integradas para usuários empresariais com pequenos volumes de dados.

(61) O valor dos motores de busca online para os seus utilizadores empresariais e finais aumenta à medida que o número total desses utilizadores aumenta. Os provedores de mecanismos de busca on-line coletam e armazenam conjuntos de dados agregados contendo informações sobre as pesquisas dos usuários e como eles interagiram com os resultados fornecidos a eles. Os provedores de mecanismos de busca on-line coletam esses dados de pesquisas realizadas em seus próprios mecanismos de busca on-line e, quando aplicável, de pesquisas realizadas nas plataformas de seus parceiros de negócios localizados mais abaixo na cadeia de valor. O acesso dos gatekeepers a esses dados sobre classificações, consultas, cliques e visualizações é uma grande barreira à entrada e expansão do mercado, prejudicando a contestabilidade dos mecanismos de busca online. Os gatekeepers devem, portanto, ser obrigados a fornecer acesso, em termos justos, razoáveis e não discriminatórios, a esses dados sobre classificações, consultas, cliques e visualizações em relação a pesquisas gratuitas e pagas realizadas por consumidores em mecanismos de busca on-line para outras empresas que fornecem esses serviços, para que essas empresas terceirizadas possam otimizar seus serviços e competir pelos serviços de plataforma principais correspondentes. Esse acesso também deve ser concedido a terceiros contratados pelos provedores de um mecanismo de busca online que atuam como processadores de dados para tais mecanismos de busca online. Ao facilitar o acesso aos seus dados de pesquisa, os guardiões devem garantir a proteção dos dados pessoais dos usuários finais, em particular contra riscos potenciais de reidentificação, por meios apropriados, como a anonimização desses dados pessoais, sem degradar substancialmente a qualidade ou a utilidade dos dados. Dados relevantes são anonimizados se os dados pessoais forem alterados irreversivelmente de tal forma que as informações não se relacionem mais com uma pessoa física identificada ou identificável ou quando os dados pessoais forem anonimizados de tal forma que o titular dos dados não seja ou não seja mais identificável.

(62) No que diz respeito às lojas de aplicações informáticas, aos motores de busca em linha e aos serviços de redes sociais em linha enumerados na decisão de designação, os controladores de acesso devem publicar e aplicar condições gerais de acesso que sejam justas, razoáveis e não discriminatórias. Essas condições gerais devem prever um mecanismo alternativo de resolução de litígios localizado na União que seja facilmente acessível, imparcial, independente e gratuito para os utilizadores profissionais, sem prejuízo dos custos a suportar pelos utilizadores profissionais e de medidas proporcionais destinadas a evitar o abuso do mecanismo de resolução de litígios por parte dos utilizadores profissionais. O mecanismo de resolução de litígios não deverá prejudicar o direito dos utilizadores profissionais de procurarem reparação junto das autoridades judiciais, em conformidade com o direito da União e o direito nacional. Em particular, os gatekeepers que fornecem acesso a lojas de aplicativos de computador são uma porta de entrada importante para usuários empresariais que buscam alcançar usuários finais. Tendo em vista o desequilíbrio no poder de barganha entre esses guardiões e os usuários profissionais de suas lojas de aplicativos de software, esses guardiões não devem ser autorizados a impor condições gerais, incluindo condições de preços, que sejam injustas ou levem a uma diferenciação injustificada.

Os preços ou outras condições gerais de acesso devem ser considerados injustos se levarem a um desequilíbrio entre os direitos dos usuários empresariais e as obrigações impostas a eles, derem aos gatekeepers uma vantagem desproporcional em relação ao serviço que eles fornecem aos usuários empresariais ou colocarem em desvantagem os usuários empresariais que fornecem serviços idênticos ou semelhantes aos oferecidos pelos gatekeepers. Os seguintes parâmetros podem servir como critérios para determinar a equidade das condições gerais de acesso: os preços cobrados ou as condições impostas por outros fornecedores de lojas de aplicações informáticas para serviços idênticos ou semelhantes; os preços cobrados ou as condições impostas pelo fornecedor da loja de aplicativos de computador para serviços semelhantes ou relacionados ou para diferentes tipos de usuários finais; os preços cobrados ou condições impostas pelo provedor da loja de aplicativos para o mesmo serviço em diferentes regiões geográficas; os preços cobrados ou condições impostas pelo provedor da loja de aplicativos para o mesmo serviço que o gatekeeper fornece a si mesmo. Esta obrigação não deve estabelecer um direito de acesso e não deve prejudicar a capacidade dos fornecedores de lojas de aplicações informáticas, motores de busca online e serviços de redes sociais online de assumirem a responsabilidade necessária no combate a conteúdos ilegais e indesejados, tal como estabelecido num regulamento sobre um mercado único de serviços digitais.

(63) Os controladores de acesso podem dificultar a capacidade dos utilizadores empresariais e dos utilizadores finais de cancelarem a subscrição de um serviço básico de plataforma ao qual tenham subscrito anteriormente. Portanto, regras devem ser estabelecidas para evitar uma situação em que os guardiões minem os direitos dos usuários empresariais e finais de escolher livremente o serviço básico de plataforma que usam. Para salvaguardar a livre escolha dos usuários profissionais e usuários finais, os gatekeepers não devem ter permissão para dificultar ou complicar desnecessariamente a vida dos usuários profissionais ou usuários finais.

finais é baixo de um serviço de plataforma básico. Fechar uma conta ou cancelar a assinatura de um serviço não deve ser mais complicado do que criar uma conta ou assinar o mesmo serviço. Os gatekeepers não devem exigir taxas adicionais ao rescindir contratos com seus usuários finais ou usuários comerciais. Os controladores de acesso devem garantir que as condições de rescisão de contratos sejam sempre proporcionais e possam ser aplicadas pelos usuários finais sem dificuldades indevidas, por exemplo, em relação aos motivos da rescisão, ao período de aviso prévio ou à forma de tal rescisão, sem prejuízo da legislação nacional aplicável, em conformidade com a legislação da União que estabelece direitos e obrigações em relação às condições de rescisão da prestação de serviços essenciais de plataforma pelos usuários finais.

- (64) A falta de interoperabilidade permite que os controladores de acesso que fornecem serviços de comunicações electrónicas relacionamentos interpessoais independentes de numeração se beneficiam de importantes efeitos de rede, o que contribui para enfraquecer a contestabilidade. Além disso, mesmo que os usuários finais optem pela multiconexão, os gatekeepers geralmente fornecem serviços de comunicações eletrónicas interpessoais independentes de número dentro de seu ecossistema de plataforma, dificultando ainda mais a entrada no mercado de provedores alternativos desses serviços e aumentando os custos para usuários finais que desejam trocar de provedor. Por conseguinte, sem prejuízo do disposto na Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho ⁽¹⁴⁾ e, em particular, as condições e procedimentos estabelecidos no seu artigo 61.º, os gatekeepers devem garantir aos prestadores terceiros de serviços de comunicações interpessoais independentes de número, gratuitamente e mediante solicitação, a interoperabilidade com determinadas funcionalidades básicas desses serviços que oferecem aos seus próprios utilizadores finais.

Os controladores de acesso devem garantir a interoperabilidade para provedores terceirizados de serviços de comunicações interpessoais independentes de número que fornecem ou pretendem fornecer seus serviços de comunicações interpessoais independentes de número a usuários finais e usuários empresariais na União. A fim de facilitar a implementação prática dessa interoperabilidade, o controlador em questão deve ser obrigado a publicar uma oferta de referência que estabeleça os detalhes técnicos e as condições gerais de interoperabilidade com seus serviços de comunicações interpessoais independentes de número. A Comissão deverá poder consultar, quando apropriado, o Organismo de Reguladores Europeus das Comunicações Eletrónicas para determinar se os detalhes técnicos e as condições gerais publicadas na oferta de referência que o controlador de acesso aplicou ou pretende aplicar garantem o cumprimento dessa obrigação.

Em todos os casos, o controlador e o fornecedor que solicita a interoperabilidade devem garantir que a interoperabilidade não comprometa um elevado nível de segurança e proteção de dados, em conformidade com as suas obrigações ao abrigo do presente regulamento e da legislação aplicável da União, em especial o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. A obrigação relativa à interoperabilidade não deverá prejudicar as informações e opções a disponibilizar aos utilizadores finais de serviços de comunicações interpessoais independentes de número de porteiro e de fornecedor que solicitem interoperabilidade ao abrigo do presente regulamento e de outros atos do direito da União, em especial o Regulamento (UE) 2016/679.

- (65) A fim de assegurar que as obrigações estabelecidas no presente regulamento sejam eficazes e limitadas ao necessário para garantir a contestabilidade e para fazer face aos efeitos nocivos das práticas desleais dos controladores de acesso, é importante defini-las e circunscrevê-las claramente, de modo a que os controladores de acesso as possam cumprir integralmente, em plena conformidade com a legislação aplicável e, em especial, com o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE, bem como com a legislação em matéria de proteção do consumidor, cibersegurança, segurança dos produtos e requisitos de acessibilidade, incluindo a Diretiva (UE) 2019/882 e a Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho ⁽¹⁵⁾. Os guardiões devem garantir o cumprimento deste Regulamento desde o início. Portanto, as medidas necessárias devem ser integradas, na medida do possível, ao design tecnológico utilizado pelos gatekeepers.

⁽¹⁴⁾ Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (JO L 321 de 17.12.2018, p. 36).

⁽¹⁵⁾ Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho, de 26 de outubro de 2016, relativa à acessibilidade dos sítios web e das aplicações móveis dos organismos do setor público (JO L 327 de 2.12.2016, p. 1).

Em alguns casos, pode ser apropriado que a Comissão, após discussões com o controlador relevante e permitindo que terceiros comentem, especifique com mais detalhes algumas das medidas que o controlador deve tomar para cumprir efetivamente com as obrigações que podem ser especificadas com mais detalhes ou, no caso de evasão, todas as obrigações. Em particular, essa especificação mais detalhada deve ser possível quando o desempenho de uma obrigação que pode ser especificada com mais detalhes puder ser afetado por variações nos serviços dentro de uma única categoria de serviços essenciais da plataforma. Para esse fim, o controlador deve poder solicitar à Comissão que inicie um processo pelo qual a Comissão possa especificar com mais detalhes algumas das medidas que o controlador deve tomar para cumprir efetivamente essas obrigações.

A Comissão deve poder decidir, a seu critério, se e quando fornecer tais especificações mais detalhadas, respeitando os princípios de igualdade de tratamento, proporcionalidade e boa administração. Nesse sentido, a Comissão deve expor as principais razões nas quais se baseia sua avaliação, incluindo as prioridades que definiu para a implementação. Este processo não deve ser utilizado para comprometer a eficácia deste Regulamento. Além disso, o processo não prejudica os poderes da Comissão para adotar uma decisão declarando o incumprimento, por parte de um controlador, das obrigações estabelecidas no presente regulamento, incluindo a possibilidade de impor multas ou sanções pecuniárias compulsórias. A Comissão deve poder reabrir um procedimento, em especial quando as medidas especificadas não se mostrarem eficazes. Quando um procedimento for reaberto devido a uma especificação ineficaz adotada por uma decisão, a Comissão deverá poder modificar a especificação prospectivamente. A Comissão também deve poder estabelecer um período razoável dentro do qual um procedimento pode ser reaberto caso as medidas especificadas não se mostrem eficazes.

- (66) Como elemento adicional para garantir a proporcionalidade, os controladores de acesso deverão ter a oportunidade de solicitar a suspensão, na medida do necessário, de uma obrigação específica em circunstâncias excepcionais fora do controlo do controlador de acesso, como uma perturbação externa imprevista que elimine temporariamente uma parte significativa da procura do utilizador final pelo serviço de plataforma essencial em causa, sempre que o controlador de acesso demonstre que o cumprimento de uma obrigação específica compromete a viabilidade económica das suas operações na União. A Comissão deve determinar as circunstâncias excepcionais que justificam a suspensão e revisá-la periodicamente para avaliar se as condições para sua concessão ainda estão reunidas.
- (67) Em circunstâncias excepcionais, justificadas por razões limitadas de saúde pública ou de segurança pública estabelecidas no direito da União e interpretadas pelo Tribunal de Justiça, a Comissão deverá poder decidir que uma determinada obrigação não se aplica a um determinado serviço essencial de plataforma. O fato de tais interesses públicos serem prejudicados pode indicar que, em certos casos excepcionais, o custo para a sociedade como um todo de fazer cumprir uma obrigação específica é muito alto e, portanto, desproporcional. Quando apropriado, a Comissão deve ser capaz de facilitar o cumprimento, determinando se é justificada uma suspensão ou uma isenção limitada e devidamente motivada. Isto deverá garantir a proporcionalidade das obrigações estabelecidas no presente regulamento sem comprometer os efeitos previstos em equidade e contestabilidade. Quando tal isenção for concedida, a Comissão deverá rever sua decisão anualmente.
- (68) Os controladores de acesso deverão informar a Comissão nos seus relatórios obrigatórios, dentro do prazo para o cumprimento das suas obrigações nos termos do presente regulamento, das medidas que implementaram ou pretendem implementar para garantir o cumprimento efetivo dessas obrigações, em especial as medidas relacionadas com o cumprimento do Regulamento (UE) 2016/679, na medida em que sejam relevantes para o cumprimento das obrigações estabelecidas no presente regulamento, o que deverá permitir à Comissão exercer as suas funções nos termos do presente regulamento. Além disso, um resumo claro, compreensível e não confidencial dessas informações deve ser disponibilizado publicamente, levando em consideração o interesse legítimo dos guardiões em proteger seus segredos comerciais e outras informações confidenciais. Essa publicação não confidencial deverá permitir que terceiros avaliem se os controladores de acesso cumprem as obrigações estabelecidas no presente regulamento. Este relatório não deverá prejudicar quaisquer medidas de execução adotadas pela Comissão em qualquer momento após a emissão do relatório. A Comissão deve publicar online um link para o resumo não confidencial do relatório, bem como para outras informações públicas baseadas nas obrigações de comunicação de informações previstas no presente regulamento, a fim de garantir que tais informações sejam totalmente acessíveis e utilizáveis, em especial para pequenas e médias empresas (doravante «PME»).

- (69) As obrigações dos controladores de acesso só deverão ser actualizadas após uma investigação exaustiva sobre a natureza e os efeitos de práticas específicas que tenham sido recentemente consideradas, na sequência de uma investigação exaustiva, desleais ou que limitem a contestabilidade da mesma forma que as práticas desleais previstas no presente regulamento e que possam ficar fora do âmbito do actual conjunto de obrigações. A Comissão deverá poder iniciar um inquérito para determinar se as obrigações existentes necessitam de ser actualizadas, quer por iniciativa própria, quer mediante pedido fundamentado de pelo menos três Estados-Membros. Ao apresentarem tais pedidos fundamentados, os Estados-Membros deverão poder incluir informações sobre ofertas de produtos, serviços, programas ou funcionalidades recentemente introduzidas que levantam questões de contestabilidade ou imparcialidade, aplicadas ou não no contexto dos serviços de plataforma principais existentes. Sempre que, após uma investigação de mercado, a Comissão considere necessário alterar elementos essenciais do presente regulamento, como a inclusão de novas obrigações que se desviem de questões de disputabilidade ou equidade já abordadas pelo presente regulamento, a Comissão deverá apresentar uma proposta de alteração do presente regulamento.
- (70) Dado o peso económico significativo dos controladores de acesso, é importante que as obrigações sejam efectivamente aplicadas e não contornadas. Para esse efeito, as regras em questão deverão aplicar-se a quaisquer práticas dos controladores de acesso, independentemente da forma que assumam ou de serem práticas contratuais, comerciais, técnicas ou quaisquer outras, na medida em que a prática corresponda aos tipos de práticas que estão sujeitas a uma das obrigações estabelecidas no presente regulamento. Os controladores de acesso não devem adotar condutas que comprometam a eficácia das proibições e obrigações estabelecidas neste Regulamento. Esse comportamento inclui o design usado pelo gatekeeper, a apresentação de opções aos usuários finais de maneira não neutra ou o uso da estrutura, função ou modo de operação de uma interface de usuário ou parte dela para interromper ou prejudicar a autonomia, a tomada de decisão ou a escolha dos usuários. Além do mais, O controlador não deve ser autorizado a se envolver em comportamentos que comprometam a interoperabilidade exigida pelo presente regulamento, por exemplo, usando medidas de proteção técnica injustificadas, termos de serviço discriminatórios, invocação de direitos autorais em interfaces de programação de aplicativos ou o fornecimento de informações enganosas. Os controladores de acesso não devem ser autorizados a evitar a sua designação através da segmentação, divisão, subdivisão, fragmentação ou separação artificial dos seus principais serviços de plataforma, a fim de contornar a aplicação dos limites quantitativos estabelecidos no presente regulamento.
- (71) A fim de assegurar a revisão eficaz do estatuto de controlador de acesso, bem como a possibilidade de ajustar a lista de serviços essenciais de plataforma fornecidos por um controlador de acesso, os controladores de acesso deverão informar a Comissão, antes de efetuarem tais aquisições, de todas as aquisições que tencionam efetuar de outras empresas que forneçam serviços essenciais de plataforma ou de quaisquer outros serviços prestados no setor digital ou de outros serviços que permitam a recolha de dados. Essas informações devem ser úteis não apenas para o processo de revisão acima mencionado sobre o status de cada controlador, mas também são cruciais para monitorar tendências mais gerais de contestabilidade no setor digital e, portanto, podem ser um fator útil a ser levado em consideração no contexto das investigações de mercado previstas no presente Regulamento. A Comissão também deve transmitir essas informações aos Estados-Membros, uma vez que podem ser utilizadas para efeitos de controlo nacional de fusões e que, em determinadas circunstâncias, a autoridade nacional competente pode remeter essas aquisições à Comissão para controlo de fusões. A Comissão também deve publicar anualmente a lista de aquisições das quais foi informada pelos gatekeepers. A fim de garantir a necessária transparência e utilidade dessas informações para os vários fins previstos no presente regulamento, os controladores de acesso devem fornecer, pelo menos, informações sobre as empresas afetadas pela concentração, o seu volume de negócios anual na União e a nível mundial, o seu âmbito de atividade, incluindo atividades diretamente relacionadas com a concentração, o valor da transação ou uma estimativa do mesmo, um resumo da concentração, incluindo a sua natureza e justificação, bem como uma lista dos Estados-Membros afetados pela transação.
- (72) Os interesses dos utilizadores finais em matéria de protecção de dados e de privacidade são relevantes para qualquer avaliação dos potenciais efeitos negativos da prática observada dos controladores de acesso para recolher e acumular grandes quantidades de dados dos utilizadores finais. Garantir um nível adequado de transparência nas práticas de definição de perfis empregadas pelos controladores de acesso, incluindo, mas não se limitando à definição de perfis na aceção do artigo 4.º(4) do Regulamento (UE) 2016/679, facilita a contestabilidade no que diz respeito aos principais serviços de plataforma. A transparência exerce pressão externa sobre os guardiões para que não tornem a criação de perfis aprofundada uma prática padrão do setor, já que potenciais participantes ou startups não conseguem acessar os dados na mesma extensão e profundidade, ou em uma escala semelhante. Maior transparência deve permitir que outras empresas que fornecem serviços essenciais de plataforma se diferenciem melhor usando melhores proteções de privacidade.

Para garantir um nível mínimo de eficácia em relação a essa obrigação de transparência, os controladores devem, pelo menos, fornecer uma descrição auditada de forma independente dos critérios nos quais a criação de perfil se baseia, incluindo se ela se baseia em dados pessoais e dados derivados da atividade do usuário, em conformidade com o Regulamento (UE) 2016/679, o processamento aplicado, a finalidade para a qual o perfil é preparado e, em última análise, usado, a duração da criação de perfil, o impacto dessa criação de perfil nos serviços dos controladores e as medidas tomadas para informar efetivamente os usuários finais sobre o uso relevante dessa criação de perfil, bem como as medidas para solicitar seu consentimento ou dar a eles a possibilidade de negá-lo ou retirá-lo. A Comissão deve encaminhar a descrição auditada ao Comité Europeu para a Proteção de Dados, a fim de auxiliar no monitoramento do cumprimento das regras de proteção de dados da União. A Comissão deverá ter poderes para desenvolver a metodologia e o procedimento para a preparação da descrição auditada, em consulta com a Autoridade Europeia para a Proteção de Dados, o Comité Europeu para a Proteção de Dados, a sociedade civil e os peritos, em conformidade com os Regulamentos (UE) n.º 1189/2008 e (UE) n.º 1189/2008, ^{qualquer}182/2011 ⁽¹⁶⁾ e (UE) 2018/1725 ⁽¹⁷⁾ do Parlamento Europeu e do Conselho.

- (73) A fim de assegurar a plena e duradoura concretização dos objetivos do presente regulamento, a Comissão deverá poder avaliar se uma empresa que presta serviços essenciais de plataforma deverá ser designada como controlador de acesso sem atingir os limiares quantitativos estabelecidos no presente regulamento; se o incumprimento sistemático por parte de um responsável justificar a imposição de medidas corretivas adicionais; se mais serviços do setor digital devem ser adicionados à lista de serviços básicos de plataforma e se práticas adicionais que são igualmente injustas e limitam a contestabilidade dos mercados digitais devem ser investigadas. Essa avaliação deve ser baseada em pesquisas de mercado realizadas dentro de um prazo apropriado, usando procedimentos e prazos claros, a fim de respaldar o efeito ex ante do presente Regulamento sobre contestabilidade e equidade no setor digital e proporcionar o necessário grau de segurança jurídica.
- (74) Na sequência de uma investigação de mercado, a Comissão deverá poder estabelecer que uma empresa que fornece um serviço essencial de plataforma satisfaz todos os critérios qualitativos gerais para ser designada como controlador de acesso. Tal empresa deverá então, em princípio, cumprir todas as obrigações relevantes estabelecidas pelo presente Regulamento. No entanto, a Comissão deve impor aos controladores de acesso designados pela Comissão como susceptíveis de gozar de uma posição consolidada e duradoura num futuro previsível apenas as obrigações que sejam necessárias e adequadas para impedir que os controladores de acesso em causa alcancem uma posição consolidada e duradoura nas suas operações. No que diz respeito a esses gatekeepers emergentes, a Comissão deve levar em conta que sua situação é, em princípio, de natureza temporária e, portanto, deve ser tomada uma decisão em um determinado momento sobre se uma empresa que fornece serviços essenciais de plataforma deve estar sujeita ao conjunto completo de obrigações aplicadas aos gatekeepers ao adquirir uma posição estabelecida e duradoura ou se as condições para a designação não são cumpridas e, portanto, todas as obrigações impostas anteriormente devem deixar de ser aplicáveis.
- (75) A Comissão deverá investigar e avaliar se se justificam medidas corretivas comportamentais adicionais ou, se for caso disso, estruturais, para garantir que os controladores de acesso não possam frustrar os objetivos do presente regulamento ao não cumprirem sistematicamente uma ou mais das obrigações nele estabelecidas. Esta situação ocorre quando a Comissão adota pelo menos três decisões de infração contra um controlador de acesso num período de oito anos, que podem estar relacionadas com diferentes serviços essenciais de plataforma e diferentes obrigações estabelecidas no presente regulamento, e quando o controlador de acesso mantém, expande ou reforça a sua importância no mercado interno, a dependência económica dos seus utilizadores empresariais e utilizadores finais dos seus serviços essenciais de plataforma, ou reforça a sua posição. Deve-se considerar que um gatekeeper manteve, expandiu ou fortaleceu sua posição quando, apesar das medidas de implementação adotadas pela Comissão, o gatekeeper continua a manter ou continuou a consolidar ou fortalecer sua importância como uma porta de entrada para usuários empresariais e usuários finais.

⁽¹⁶⁾ Regulamento (UE) n.º ^{qualquer}182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

⁽¹⁷⁾ Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, pelos órgãos e organismos da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 1725/2018, ^{qualquer}45/2001 e Decisão n.º ^{qualquer}1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

A Comissão deve ter o poder, nesses casos, de impor qualquer medida corretiva, seja comportamental ou estrutural, tendo devidamente em conta o princípio da proporcionalidade. Nesse contexto, desde que a medida corretiva seja proporcional e necessária para manter ou restaurar a imparcialidade e a contestabilidade que foram afetadas pela não conformidade sistemática, a Comissão deve ter o poder de proibir o controlador, por um período limitado, de participar de uma concentração relativa a serviços essenciais de plataforma ou outros serviços prestados no setor digital ou serviços que permitam a coleta de dados que tenham sido afetados pela não conformidade sistemática. Para permitir o envolvimento efetivo de terceiros e a possibilidade de testar medidas corretivas antes de sua implementação, a Comissão deve publicar um resumo detalhado e não confidencial do caso e das medidas a serem tomadas. A Comissão deve poder reabrir um procedimento, em especial quando as medidas corretivas especificadas se revelarem ineficazes. Quando um procedimento for reaberto devido à ineficácia das medidas corretivas adotadas por uma decisão, a Comissão deverá poder modificar essas medidas prospectivamente. A Comissão também deve poder estabelecer um período razoável dentro do qual seja possível reabrir um procedimento caso as medidas corretivas se revelem ineficazes.

(76) Sempre que um controlador de acesso, durante uma investigação sobre um incumprimento sistemático, se oferecer para assumir compromissos perante a Comissão, a Comissão deverá poder adotar uma decisão que converta esses compromissos em compromissos vinculativos para o controlador de acesso em causa, se considerar que os compromissos asseguram o cumprimento efetivo das obrigações estabelecidas no presente regulamento. Tal decisão também deve declarar que a Comissão não tem mais motivos para agir em relação à não conformidade sistemática sob investigação. Ao avaliar se os compromissos que o controlador de acesso se propôs a assumir são suficientes para garantir o cumprimento efetivo das obrigações previstas no presente regulamento, a Comissão deverá poder ter em conta as provas apresentadas pelo controlador de acesso para demonstrar a eficácia desses compromissos na prática. A Comissão deve verificar se a decisão sobre os compromissos é integralmente respeitada e atinge os seus objetivos, e deve poder reabrir a decisão se considerar que os compromissos não são eficazes.

(77) Os serviços no sector digital e os tipos de práticas relacionadas com esses serviços podem mudar rapidamente e em grande medida. A fim de garantir que este Regulamento permaneça atualizado e constitua uma resposta regulamentar eficaz e holística aos problemas levantados pelos controladores de acesso, é importante prever uma revisão regular das listas de serviços essenciais de plataforma, bem como das obrigações previstas no presente Regulamento. Isso é particularmente importante para garantir a deteção de uma prática que possa limitar a contestabilidade de serviços básicos de plataforma ou que seja injusta. Dado que o setor digital está mudando dinamicamente, embora seja importante conduzir uma revisão regular para garantir a segurança jurídica em relação às condições regulatórias, todas as revisões devem ser conduzidas dentro de um prazo razoável e apropriado. As investigações de mercado também devem garantir que a Comissão tenha uma base probatória sólida que lhe permita avaliar se deve propor a alteração deste Regulamento para rever, alargar ou elaborar as listas de serviços essenciais de plataforma. Devem também garantir que a Comissão dispõe de uma base probatória sólida para avaliar se é adequado propor a alteração das obrigações estabelecidas no presente regulamento ou adotar um ato delegado que atualize essas obrigações.

(78) No que diz respeito à conduta dos controladores de acesso aos quais as obrigações estabelecidas no presente regulamento não se aplicam, a Comissão deverá ter a possibilidade de abrir uma investigação de mercado sobre novos serviços e novas práticas, a fim de determinar se as obrigações estabelecidas no presente regulamento devem ser complementadas por um ato delegado abrangido pelo âmbito da habilitação prevista para tais atos delegados no presente regulamento, ou pela apresentação de uma proposta de alteração do presente regulamento. Isto não prejudica a possibilidade de a Comissão, em casos adequados, iniciar um procedimento nos termos do artigo 101.º ou 102.º do TFUE. Esses procedimentos devem ser desenvolvidos de acordo com o Regulamento (CE) n.º ^{qualquer}1/2003 do Conselho ⁽¹⁸⁾. Em casos de urgência justificados pelo risco de danos graves e irreparáveis à concorrência, a Comissão deverá considerar a adoção de medidas cautelares em conformidade com o artigo 8.º do Regulamento (CE) n.º 1189/2008, ^{qualquer}1/2003.

(18) Regulamento (CE) n.º ^{qualquer}1/2003 do Conselho, de 16 de Dezembro de 2002, relativa à execução das regras de concorrência estabelecidas nos artigos 81.º e 82.º do Tratado (JO L 1 de 4.1.2003, p. 1).

- (79) Sempre que os controladores de acesso recorram a práticas desleais ou a práticas que limitem a disputabilidade de serviços essenciais de plataforma já designados ao abrigo do presente regulamento, mas não expressamente previstos nas obrigações nele estabelecidas, a Comissão deverá poder atualizar o presente regulamento por meio de atos delegados. Tais atualizações por meio de ato delegado devem estar sujeitas aos mesmos critérios de pesquisa e, portanto, devem ser precedidas de uma investigação de mercado. A Comissão também deve aplicar um critério predefinido para detectar tais tipos de práticas. Este critério legal deve garantir que o tipo de obrigações que os controladores de acesso podem enfrentar a qualquer momento ao abrigo do presente regulamento sejam suficientemente previsíveis.
- (80) A fim de assegurar a aplicação e o cumprimento efetivos do presente regulamento, a Comissão deverá dispor de fortes poderes de investigação e de execução que lhe permitam investigar, aplicar e monitorizar as regras estabelecidas no presente regulamento, assegurando simultaneamente o respeito pelo direito fundamental de ser ouvido e de ter acesso ao processo no contexto dos processos de execução. A Comissão deverá ter estes poderes de investigação também para realizar investigações de mercado, em particular com o objetivo de atualizar e rever o presente regulamento.
- (81) A Comissão deverá ter o poder de solicitar as informações necessárias para efeitos do presente regulamento. Em particular, a Comissão deve ter acesso a documentos, dados, bases de dados, algoritmos e informações relevantes necessários para iniciar e realizar investigações e para monitorizar o cumprimento das obrigações estabelecidas no presente regulamento, independentemente de quem detém essas informações e qualquer que seja a sua forma ou formato, o seu meio de armazenamento e o local onde são armazenadas.
- (82) A Comissão deverá poder solicitar directamente às empresas ou associações de empresas que forneçam todas as provas, dados e informações relevantes. Além disso, a Comissão deverá poder solicitar qualquer informação relevante às autoridades competentes do Estado-Membro, ou a qualquer pessoa singular ou coletiva para efeitos do presente regulamento. De acordo com uma decisão da Comissão, as empresas são obrigadas a responder perguntas factuais e fornecer documentos.
- (83) A Comissão deverá também ter poderes para efectuar inspecções a qualquer empresa ou associação de empresas, para entrevistar qualquer pessoa que possa ter informações úteis e para registar as suas declarações.
- (84) As medidas provisórias podem ser um instrumento importante para garantir que, enquanto uma investigação estiver em curso, a infração sob investigação não cause danos graves e irreparáveis aos utilizadores profissionais ou aos utilizadores finais dos controladores de acesso. Este instrumento é importante para evitar alterações que poderiam ser muito difíceis de desfazer por uma decisão tomada pela Comissão no final do procedimento. A Comissão deverá, por conseguinte, ter o poder de ordenar medidas cautelares no contexto de um procedimento iniciado com vista à possível adoção de uma decisão de infração. Este poder deve ser exercido nos casos em que a Comissão tenha constatado a primeira vista uma violação das obrigações dos guardiões e onde existe o risco de os utilizadores profissionais ou utilizadores finais dos guardiões poderem sofrer danos graves e irreparáveis. As medidas provisórias devem ser aplicadas apenas por um período específico, até o final do procedimento, quando a Comissão conclui o processo, ou por um período específico que pode ser renovado na medida necessária e apropriada.
- (85) A Comissão deverá poder tomar as medidas necessárias para monitorizar a aplicação efectiva e o cumprimento das obrigações estabelecidas no presente regulamento. Essas medidas devem incluir a capacidade da Comissão de nomear peritos e auditores externos independentes para auxiliar a Comissão nesse processo, inclusive, quando apropriado, dentre as autoridades competentes dos Estados-Membros, como autoridades de proteção de dados ou autoridades de defesa do consumidor. No que diz respeito à nomeação de auditores, a Comissão deve garantir uma rotatividade suficiente.

- (86) O cumprimento das obrigações impostas pelo presente regulamento deverá ser assegurado através de multas e de sanções pecuniárias compulsórias. Para esse efeito, devem também ser fixados níveis adequados de multas e sanções pecuniárias compulsórias por incumprimento de obrigações e violação de regras processuais, sujeitos a prazos de prescrição adequados, em conformidade com os princípios da proporcionalidade e da equidade. Ninguém menos que o mesmo. A Comissão e as autoridades nacionais relevantes devem coordenar seus esforços de execução para garantir o respeito a esses princípios. Em especial, a Comissão deverá ter em conta todas as multas e sanções pecuniárias compulsórias impostas à mesma pessoa coletiva pelos mesmos factos, através de uma decisão final em processos relativos a uma infração de outras regras nacionais ou da União, a fim de garantir que o total de multas e sanções pecuniárias compulsórias impostas corresponde à gravidade das infrações cometidas.
- (87) A fim de garantir a cobrança efectiva das multas impostas às associações empresariais por infrações que cometeram, é necessário estabelecer as condições em que a Comissão poderá exigir o pagamento da coima aos membros da associação de empresas quando esta for insolvente.
- (88) No âmbito dos procedimentos efectuados nos termos do presente regulamento, deverá ser concedido à empresa em causa o direito de ser ouvida pela Comissão e as decisões tomadas deverão ser amplamente divulgadas. Ao mesmo tempo em que se garante o direito à boa administração, o direito de acesso ao processo e o direito de ser ouvido, é essencial proteger as informações confidenciais. Além disso, respeitando a confidencialidade das informações, a Comissão deve garantir que qualquer informação na qual a decisão se baseia seja comunicada de tal forma que o destinatário da decisão possa compreender os fatos e considerações que levaram à decisão. Também é necessário garantir que a Comissão utilize apenas as informações coletadas de acordo com o presente regulamento para os fins do mesmo, salvo disposição específica em contrário. Por fim, deve ser possível, sob certas condições, que alguns documentos profissionais, como comunicações entre advogados e seus clientes, sejam considerados confidenciais se as condições relevantes forem atendidas.
- (89) Ao preparar resumos não confidenciais para publicação, a fim de permitir efetivamente que terceiros interessados apresentem comentários, a Comissão deverá ter devidamente em conta o interesse legítimo das empresas na proteção dos seus segredos comerciais e de outras informações confidenciais.
- (90) A aplicação coerente, eficaz e complementar dos instrumentos jurídicos disponíveis aplicáveis aos controladores de acesso exige cooperação e coordenação entre a Comissão e as autoridades nacionais, dentro dos limites das respectivas competências. A Comissão e as autoridades nacionais devem cooperar e coordenar as ações necessárias para implementar os instrumentos jurídicos disponíveis para os controladores de acesso, na aceção do presente regulamento, e respeitar o princípio da cooperação leal estabelecido no artigo 4.º do Tratado da União Europeia (TUE). As autoridades nacionais deverão poder apoiar a Comissão, fornecendo-lhe todas as informações necessárias na sua posse ou auxiliando-a, mediante solicitação, no exercício dos seus poderes, a fim de permitir que a Comissão desempenhe melhor as tarefas que lhe são conferidas pelo presente regulamento.
- (91) A Comissão é a única autoridade competente para fazer cumprir o presente regulamento. A fim de apoiar a Comissão, os Estados-Membros devem poder autorizar as suas autoridades nacionais competentes em matéria de concorrência a realizar investigações sobre possíveis violações, por parte dos controladores de acesso, de determinadas obrigações ao abrigo do presente regulamento. Em particular, isso pode ser relevante em casos em que não seja possível determinar com base na questão de saber se a conduta de um controlador de acesso pode constituir uma violação do presente regulamento, das regras de concorrência que a autoridade nacional competente tem poderes para aplicar, ou de ambos. A autoridade nacional competente para a aplicação da lei da concorrência deverá informar a Comissão das suas conclusões sobre o possível incumprimento, por parte dos controladores de acesso, de determinadas obrigações ao abrigo do presente regulamento, com vista a que a Comissão, enquanto única autoridade com poderes para aplicar as disposições estabelecidas no presente regulamento, inicie um procedimento para investigar qualquer incumprimento.

A Comissão deve ter total discricção para decidir sobre o início de tais procedimentos. A fim de evitar a sobreposição de investigações ao abrigo do presente regulamento, a autoridade nacional competente em causa deverá informar a Comissão, antes de empreender a primeira medida de investigação, sobre um possível incumprimento, por parte dos controladores de acesso, de determinadas obrigações ao abrigo do presente regulamento. Além disso, as autoridades nacionais competentes devem cooperar e coordenar-se estreitamente com a Comissão na aplicação das regras nacionais de concorrência aos controladores de acesso, em especial no que diz respeito ao cálculo do montante das sanções. Para esse efeito, devem informar a Comissão quando iniciarem procedimentos baseados nas regras nacionais de concorrência contra os controladores de acesso, bem como antes de imporem obrigações aos controladores de acesso nesses procedimentos. A fim de evitar duplicações, as informações relativas ao projeto de decisão nos termos do artigo 11.º do Regulamento (CE) n.º ^{qualquer}1/2003 deverá poder servir, quando adequado, como uma notificação ao abrigo do presente regulamento.

- (92) A fim de proteger a aplicação e a execução harmonizadas do presente regulamento, é importante assegurar que as autoridades nacionais, em especial os tribunais nacionais, disponham de todas as informações necessárias para garantir que as suas decisões não entrem em conflito com uma decisão tomada pela Comissão nos termos do presente regulamento. Os tribunais nacionais deverão ser autorizados a solicitar à Comissão que lhes transmita informações ou pareceres sobre questões relacionadas com a aplicação do presente regulamento. Ao mesmo tempo, a Comissão deve poder apresentar observações orais ou escritas aos tribunais nacionais. Isto não prejudica o direito dos tribunais nacionais de solicitarem uma decisão prejudicial com base no artigo 267.º do TFUE.
- (93) A fim de assegurar a coerência e a complementaridade efetiva na aplicação do presente regulamento e de outras regras setoriais aplicáveis aos controladores de acesso, a Comissão deverá beneficiar dos conhecimentos especializados de um grupo específico de alto nível. Este grupo de alto nível deverá também poder prestar assistência à Comissão, prestando aconselhamento, conhecimentos especializados e recomendações, sempre que adequado, sobre questões gerais relacionadas com a aplicação ou execução do presente regulamento. O grupo de alto nível deve ser composto por organismos e redes europeias relevantes, e sua composição deve garantir um alto nível de especialização e equilíbrio geográfico. Os membros do grupo de alto nível devem informar regularmente as agências e redes que representam sobre o trabalho realizado no âmbito do grupo e consultá-las a esse respeito.
- (94) Uma vez que as decisões tomadas pela Comissão ao abrigo do presente regulamento estão sujeitas a revisão pelo Tribunal de Justiça, em conformidade com o TFUE, nos termos do artigo 261.º do Tratado, o Tribunal de Justiça deverá ter plena jurisdição sobre as coimas e as sanções pecuniárias compulsórias.
- (95) A Comissão deverá poder elaborar orientações para fornecer orientações adicionais sobre diferentes aspetos do presente regulamento ou para apoiar as empresas que prestam serviços essenciais de plataforma no cumprimento das obrigações previstas no presente regulamento. Essas orientações podem basear-se, em particular, na experiência adquirida pela Comissão na monitorização do cumprimento do presente regulamento. A publicação de orientações nos termos do presente regulamento é uma prerrogativa e permanece ao critério exclusivo da Comissão e não deve ser considerada um elemento constitutivo para garantir que a empresa ou associações de empresas em causa cumpram as suas obrigações ao abrigo do presente regulamento.
- (96) A utilização de normas técnicas pode facilitar o cumprimento de algumas das obrigações dos controladores de acesso, como as relacionadas com o acesso aos dados, a portabilidade dos dados ou a interoperabilidade. A este respeito, sempre que adequado e necessário, a Comissão deverá poder solicitar às organizações europeias de normalização que as desenvolvam.
- (97) A fim de garantir a equidade e a disputabilidade dos mercados no setor digital em que os controladores de acesso estão presentes em toda a União, o poder de adotar atos em conformidade com o artigo 290.º do TFUE deverá ser delegado na Comissão no que diz respeito à alteração da metodologia para determinar se os limiares quantitativos para utilizadores finais ativos e utilizadores empresariais ativos para a designação de controladores de acesso são cumpridos, tal como estabelecido num anexo ao presente regulamento, no que diz respeito à especificação mais aprofundada dos elementos adicionais da metodologia não incluídos nesse anexo para determinar se os limiares quantitativos para a designação de controladores de acesso são cumpridos, e no que diz respeito à complementação das obrigações existentes estabelecidas no presente regulamento quando, com base numa investigação de mercado, a Comissão determinou a necessidade de atualizar as obrigações para abordar práticas que limitam a disputabilidade dos principais serviços de plataforma ou que são desleais e a atualização em consideração enquadra-se no âmbito dos poderes estabelecidos para tais atos delegados no presente regulamento.

- (98) Ao adotar atos delegados nos termos do presente regulamento, é particularmente importante que a Comissão proceda às consultas adequadas durante os seus trabalhos preparatórios, inclusive a nível de peritos, e que essas consultas sejam conduzidas em conformidade com os princípios estabelecidos no Acordo Interinstitucional de 13 de abril de 2016 sobre legislar melhor ⁽¹⁹⁾. Em particular, para garantir a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os seus peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratam da preparação de atos delegados.
- (99) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão para especificar as medidas a pôr em prática pelos controladores de acesso, a fim de cumprir eficazmente as obrigações previstas no presente regulamento; suspender, no todo ou em parte, uma obrigação específica imposta a um guardião; isentar, no todo ou em parte, um porteiro de uma obrigação específica; especificar as medidas a aplicar por um controlador de acesso quando este contorna as obrigações estabelecidas no presente regulamento; pesquisa de mercado completa para nomear um gatekeeper; impor medidas corretivas em caso de não conformidade sistemática; ordenar medidas cautelares contra um porteiro; tornar compromissos vinculativos para um guardião; declarar um default; fixar o valor final da multa compulsória; determinar a forma, o conteúdo e outros detalhes das notificações, envios de informações, solicitações fundamentadas e relatórios regulatórios enviados pelos gatekeepers; estabelecer disposições operacionais e técnicas com vista à implementação da interoperabilidade, bem como a metodologia e o procedimento para a descrição auditada das técnicas utilizadas para a definição de perfis dos consumidores; estabelecendo disposições práticas para procedimentos, prorrogação de prazos, exercício de direitos durante procedimentos e condições de divulgação, bem como para cooperação e coordenação entre a Comissão e as autoridades nacionais. Esses poderes devem ser exercidos de acordo com o Regulamento (UE) n.º ^{qualquer}182/2011.
- (100) O procedimento de exame deverá ser utilizado para a adoção de um ato de execução sobre as disposições práticas de cooperação e coordenação entre a Comissão e os Estados-Membros. O procedimento consultivo deverá ser utilizado para os outros atos de execução previstos no presente regulamento, uma vez que esses atos de execução dizem respeito a aspetos práticos dos procedimentos estabelecidos no presente regulamento, tais como a forma, o conteúdo e outros detalhes das várias fases do procedimento, as modalidades práticas das várias fases do procedimento, tais como, por exemplo, a prorrogação dos prazos processuais ou o direito de ser ouvido, bem como decisões de execução individuais endereçadas ao controlador de acesso.
- (101) De acordo com o Regulamento (UE) n.º ^{qualquer}182/2011, cada Estado-Membro deve estar representado no comité consultivo e decidir a composição da sua delegação. A delegação pode incluir, entre outros, peritos das autoridades competentes dos Estados-Membros que tenham conhecimentos especializados relevantes sobre uma questão específica submetida ao comité consultivo.
- (102) Os reclamantes podem levar ao conhecimento das autoridades competentes novas informações que as ajudem a detectar infrações ao presente regulamento e lhes permitam impor sanções. Devem ser assegurados mecanismos adequados para permitir que os denunciante alertem as autoridades competentes sobre violações reais ou potenciais do presente regulamento e para os proteger de retaliações. Para o efeito, deverá prever-se no presente regulamento que a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho ⁽²⁰⁾ aplica-se à denúncia de violações do presente regulamento e à proteção das pessoas que denunciam tais violações.
- (103) A fim de aumentar a segurança jurídica, a aplicabilidade, ao abrigo do presente regulamento, da referida diretiva à comunicação de infrações ao presente regulamento e à proteção das pessoas que comunicam tais infrações deverá ser refletida na Diretiva (UE) 2019/1937. É, portanto, adequado alterar o anexo da Diretiva (UE) 2019/1937 em conformidade. Cabe aos Estados-Membros garantir que tal alteração seja refletida nas suas medidas de transposição adotadas nos termos da Diretiva (UE) 2019/1937, embora a adoção de medidas nacionais de transposição não seja uma condição para a aplicabilidade dessa diretiva à comunicação de infrações ao presente regulamento e à proteção das pessoas que comunicam tais infrações a partir da data de aplicação do presente regulamento.

⁽¹⁹⁾ JO L 123 de 12.5.2016, p. 1.

⁽²⁰⁾ Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (JO L 305 de 26.11.2019, p. 17).

- (104) Os consumidores deverão poder fazer valer os seus direitos relativamente às obrigações impostas aos controladores de acesso ao abrigo do presente regulamento através de ações coletivas, em conformidade com a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho ⁽²¹⁾. Para o efeito, o presente regulamento deve prever que a Diretiva (UE) 2020/1828 se aplica às ações coletivas intentadas contra atos de controladores de acesso que violem as disposições do presente regulamento e prejudiquem ou sejam suscetíveis de prejudicar os interesses coletivos dos consumidores. É, por conseguinte, adequado alterar o anexo dessa diretiva em conformidade. Cabe aos Estados-Membros garantir que tal alteração seja refletida nas suas medidas de transposição adotadas nos termos da Diretiva (UE) 2020/1828, embora a adoção de medidas nacionais de transposição a este respeito não seja uma condição para a aplicabilidade dessa diretiva às ações coletivas. A aplicabilidade da Diretiva (UE) 2020/1828 às ações representativas movidas contra atos de controladores de acesso que violem as disposições do presente regulamento e prejudiquem ou sejam suscetíveis de prejudicar os interesses coletivos dos consumidores deve começar a partir da data de aplicação das disposições legislativas, regulamentares e administrativas dos Estados-Membros necessárias para transpor essa diretiva, ou a partir da data de aplicação do presente regulamento, consoante a que ocorrer mais tarde.
- (105) A Comissão deverá avaliar regularmente o presente regulamento e monitorizar de perto os seus efeitos na disputabilidade e na equidade das relações comerciais na economia das plataformas em linha, em especial com vista a determinar se necessita de ser alterado à luz dos desenvolvimentos tecnológicos ou comerciais relevantes. Esta avaliação deve incluir uma revisão regular da lista de serviços essenciais da plataforma e das obrigações endereçadas aos guardiões, bem como da sua aplicação, com vista a garantir que os mercados digitais em toda a União sejam contestáveis e justos. Nesse contexto, a Comissão deverá também avaliar o âmbito da obrigação relativa à interoperabilidade dos serviços de comunicações interpessoais independentes do número. Para obter uma visão geral abrangente da evolução do setor digital, a avaliação deve levar em consideração as experiências dos Estados-Membros e das partes interessadas relevantes. A este respeito, a Comissão também deve poder levar em consideração os pareceres e relatórios que lhe são submetidos pelo Observatório da Economia das Plataformas Online, criado pela Decisão da Comissão C(2018)2393 de 26 de abril de 2018. Após a sua avaliação, a Comissão deve tomar as medidas adequadas. Ao realizar avaliações e revisões das práticas e obrigações estabelecidas no presente regulamento, a Comissão deverá procurar manter um elevado nível de proteção e respeito pelos direitos e valores comuns, em especial a igualdade e a não discriminação.
- (106) Sem prejuízo do processo orçamental e através dos instrumentos financeiros existentes, deverão ser atribuídos à Comissão recursos humanos, financeiros e técnicos suficientes para garantir que esta possa desempenhar eficazmente as suas funções e exercer os seus poderes no que diz respeito ao controlo do cumprimento do presente regulamento.
- (107) Atendendo a que o objetivo do presente regulamento, nomeadamente garantir a disputabilidade e a equidade no setor digital em geral e nos serviços essenciais de plataforma em particular, a fim de promover a inovação, produtos e serviços digitais de elevada qualidade, preços justos e competitivos, variedade e elevada qualidade para os utilizadores finais no setor digital, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido ao modelo de negócio e às operações dos controladores de acesso, bem como à escala e aos efeitos destes, ser mais bem alcançado ao nível da União, a União pode adotar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade estabelecido no mesmo artigo, o presente regulamento não excede o necessário para atingir esse objetivo.
- (108) A Autoridade Europeia para a Proteção de Dados, consultada nos termos do artigo 42.º do Regulamento (UE) 2018/1725, emitiu o seu parecer em 10 de fevereiro de 2021 ⁽²²⁾.
- (109) O presente regulamento respeita os direitos fundamentais e observa os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, em especial nos seus artigos 16.º, 47.º e 50.º. Consequentemente, a interpretação e a aplicação do presente regulamento deverão respeitar esses direitos e princípios.

⁽²¹⁾ Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativa a ações coletivas para proteção dos interesses coletivos dos consumidores e que revoga a Diretiva 2009/22/CE (JO L 409 de 4.12.2020, p. 1).

⁽²²⁾ DO C 147 de 26.4.2021, p. 4.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

OBJETIVO, ÂMBITO DE APLICAÇÃO E DEFINIÇÕES

Artigo 1

Objeto e âmbito de aplicação

1. O objetivo do presente regulamento é contribuir para o bom funcionamento do mercado interno, estabelecendo regras harmonizadas para garantir mercados justos e contestáveis no setor digital, onde existam controladores para todas as empresas em toda a União, em benefício tanto das empresas como dos utilizadores finais.

2. O presente regulamento aplica-se aos serviços essenciais de plataforma prestados ou oferecidos pelos controladores de acesso a utilizadores profissionais estabelecidos na União ou a utilizadores finais estabelecidos ou localizados na União, independentemente do local de estabelecimento ou residência dos controladores de acesso e da legislação aplicável à prestação do serviço.

3. O presente regulamento não se aplica aos mercados relacionados com:

(a) redes de comunicações eletrónicas, tal como definidas no artigo 2.º, ponto 1, da Diretiva (UE) 2018/1972;

(b) serviços de comunicações eletrónicas, tal como definidos no ponto 4 do artigo 2.º da Diretiva (UE) 2018/1972, exceto os relativos a serviços de comunicações interpessoais independentes do número.

4. No que diz respeito aos serviços de comunicações interpessoais, tal como definidos no ponto (5) do artigo 2.º da Diretiva (UE) 2018/1972, o presente regulamento não prejudica os poderes e responsabilidades conferidos às autoridades reguladoras nacionais e a outras autoridades competentes nos termos do artigo 61.º dessa diretiva.

5. A fim de evitar a fragmentação do mercado interno, os Estados-Membros não imporão obrigações adicionais aos controladores de acesso por meio de leis, regulamentos ou disposições administrativas destinadas a garantir mercados disputáveis e justos. Nada no presente regulamento impede os Estados-Membros de imporem obrigações às empresas, incluindo as empresas que prestam serviços essenciais de plataforma, relacionadas com questões fora do âmbito do presente regulamento, desde que essas obrigações sejam compatíveis com o direito da União e não decorram da consideração das empresas em causa como controladores de acesso na aceção do presente regulamento.

6. O presente regulamento não prejudica a aplicação dos artigos 101.º e 102.º do TFUE. Entende-se também sem prejuízo da aplicação de:

(a) regras nacionais de concorrência que proibam acordos anticoncorrenciais, decisões de associações de empresas, práticas concertadas e abusos de posições dominantes;

(b) regras nacionais de concorrência que proibam outras formas de conduta unilateral na medida em que se apliquem a empresas que não sejam controladores de acesso ou que equivalham à imposição de obrigações adicionais aos controladores de acesso, e

c) Regulamento (CE) n.º ^{qualquer}139/2004 do Conselho ⁽²³⁾ e regras nacionais sobre controle de concentração.

(23) Regulamento (CE) n.º ^{qualquer}Regulamento (CE) n.º 139/2004 do Conselho, de 20 de janeiro de 2004, relativo ao controlo das concentrações de empresas («Regulamento Comunitário das Concentrações») (JO L 24 de 29.1.2004, p. 1).

7. As autoridades nacionais não devem tomar decisões contrárias a uma decisão tomada pela Comissão nos termos do presente regulamento. A Comissão e os Estados-Membros devem trabalhar em estreita cooperação e coordenar as suas medidas de execução com base nos princípios estabelecidos nos artigos 37.º e 38.º.

Artigo 2

Definições

Para efeitos do presente regulamento, entende-se por:

- 1) «gatekeeper» significa uma empresa que fornece serviços básicos de plataforma, designada de acordo com o artigo 3.º;
- 2) «serviço de plataforma principal» significa qualquer um dos seguintes:
 - a) serviços de intermediação on-line;
 - b) motores de busca online;
 - c) serviços de redes sociais online;
 - d) serviços de plataforma de partilha de vídeos;
 - e) serviços de comunicações interpessoais independentes de número;
 - f) sistemas operacionais;
 - g) navegadores da web;
 - h) assistentes virtuais;
 - i) serviços de computação em nuvem;
 - (j) serviços de publicidade online, incluindo redes de publicidade, plataformas de troca de publicidade e quaisquer outros serviços de intermediação de publicidade, fornecidos por uma empresa que forneça qualquer um dos serviços básicos de plataforma listados nos pontos (a) a (i);
- 3) «serviço da sociedade da informação» significa qualquer «serviço» tal como definido no artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535;
- 4) «setor digital» significa o setor de produtos fornecidos e serviços prestados por ou através de serviços da sociedade da informação;
- 5) «serviços de intermediação em linha» significa «serviços de intermediação em linha» tal como definidos no ponto (2) do artigo 2.º do Regulamento (UE) 2019/1150;
- 6) «motor de busca em linha» significa um «motor de busca em linha» tal como definido no ponto 5 do artigo 2.º do Regulamento (UE) 2019/1150;
- 7) «serviço de rede social online» significa uma plataforma que permite aos utilizadores finais ligarem-se e comunicarem entre si, partilharem conteúdos e descobrirem conteúdos e outros utilizadores através de vários dispositivos, e em particular através de chats, publicações, vídeos e recomendações;
- 8) «serviço de plataforma de partilha de vídeos» significa um «serviço de plataforma de partilha de vídeos» tal como definido no artigo 1.º, n.º 1, alínea a).Bis), da Diretiva 2010/13/UE;
- 9) «serviço de comunicações interpessoais independente do número» significa um «serviço de comunicações interpessoais independente do número», tal como definido no ponto 7 do artigo 2.º da Diretiva (UE) 2018/1972;
- 10) «sistema operacional», Programa sistema que controla as funções básicas do equipamento e do Programa e permite que aplicativos de computador sejam executados nele;
- 11) «navegador da web» significa um aplicativo de computador que permite aos usuários finais acessar e interagir com conteúdo da web hospedado em servidores conectados a redes como a Internet, incluindo navegadores da web independentes e navegadores da web integrados à Internet. Programa similar;

- 12) "assistente virtual" significa um Programa que pode processar solicitações, tarefas ou perguntas, incluindo aquelas formuladas por meio de sons, imagens, texto, gestos ou movimentos e que, com base nessas solicitações, tarefas ou perguntas, fornece acesso a outros serviços ou controla dispositivos físicos conectados;
- 13) «serviço de computação em nuvem» significa um «serviço de computação em nuvem» tal como definido no ponto 19 do artigo 4.º da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ⁽²⁴⁾;
- 14) «lojas de aplicações» significa um tipo de serviço de intermediação online centrado em aplicações informáticas como um produto ou serviço intermediário;
- 15) «aplicação informática» significa qualquer produto ou serviço digital que seja executado num sistema operativo;
- 16) «serviço de pagamento» significa um «serviço de pagamento» tal como definido no ponto (3) do artigo 4.º da Diretiva (UE) 2015/2366;
- 17) «serviço de apoio técnico para um serviço de pagamento» significa um serviço na acepção do artigo 3.º, alínea j), da Directiva (UE) 2015/2366;
- 18) 'sistema de pagamento de compras no aplicativo' significa um aplicativo de computador, serviço ou interface de usuário que facilita a compra de conteúdo digital ou serviços digitais dentro de um aplicativo de computador, como conteúdo, assinaturas, recursos ou funcionalidades, e o pagamento por tais compras;
- 19) «serviço de identificação» significa um tipo de serviço fornecido em conjunto com ou em apoio aos serviços essenciais da plataforma que permite qualquer tipo de verificação da identidade dos utilizadores finais ou dos utilizadores empresariais, independentemente da tecnologia utilizada;
- 20) "usuário final" significa qualquer pessoa física ou jurídica que utilize os serviços básicos da plataforma e que não o faça como usuário profissional;
- 21) «utilizador profissional» significa qualquer pessoa singular ou coletiva que, numa base comercial ou profissional, utilize serviços essenciais da plataforma para fornecer produtos ou prestar serviços a utilizadores finais ou utilize esses serviços no contexto do fornecimento de produtos ou da prestação de serviços a utilizadores finais;
- (22) «classificação» significa a proeminência relativa atribuída a produtos ou serviços oferecidos através de serviços de intermediação em linha, serviços de redes sociais em linha, serviços de plataformas de partilha de vídeos ou assistentes virtuais, ou a relevância atribuída aos resultados de pesquisa por motores de busca em linha, tal como apresentados, organizados ou comunicados por empresas que prestam serviços de intermediação em linha, serviços de redes sociais em linha, serviços de plataformas de partilha de vídeos, assistentes virtuais ou motores de busca em linha, independentemente dos meios tecnológicos utilizados para tal apresentação, organização ou comunicação e independentemente de ser apresentado ou comunicado apenas um resultado;
- 23) "resultados de pesquisa" significa qualquer informação em qualquer formato, incluindo resultados textuais, gráficos, de voz ou outros, oferecidos em resposta e em relação a uma consulta de pesquisa, independentemente de a informação oferecida ser um resultado pago ou não pago, uma resposta direta ou qualquer produto, serviço ou informação oferecida em conexão com, exibida em conjunto com, ou integrada em parte ou totalmente em resultados orgânicos;
- 24) «dados» significa qualquer representação digital de atos, factos ou informações e qualquer compilação de tais atos, factos ou informações, incluindo na forma de uma gravação sonora, visual ou audiovisual;
- 25) «dados pessoais» significa «dados pessoais» tal como definidos no ponto 1 do artigo 4.º do Regulamento (UE) 2016/679;
- 26) «dados não pessoais» significa dados que não são dados pessoais;
- 27) «empresa» significa uma entidade que exerce uma atividade económica, independentemente do seu estatuto jurídico e do modo como é financiada, incluindo todas as empresas relacionadas ou ligadas que formam um grupo através do controlo direto ou indireto de uma empresa por outra;

⁽²⁴⁾ 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 dos sistemas de informação em toda a União (JO L 194 de 19.7.2016, p. 1).

- 28) «controlo» significa a capacidade de exercer influência decisiva sobre uma empresa, na acepção do artigo 3.º, n.º 2, do Regulamento (CE) n.º 1089/2008, qualquer 139/2004;
- 29) «interoperabilidade» significa a capacidade de trocar informações e de utilizar mutuamente as informações que foram trocadas através de interfaces ou outras soluções, de modo a que todos os elementos de ferragens qualquer Programas trabalhar com ferragens Programas diferente e com os usuários em todas as formas em que eles devem trabalhar;
- 30) «volume de negócios» significa os montantes obtidos por uma empresa na acepção do artigo 5.º, n.º 1, do Regulamento (CE) n.º 107/2008, qualquer 139/2004;
- 31) «criação de perfis» significa «criação de perfis» tal como definido no ponto (4) do artigo 4.º do Regulamento (UE) 2016/679;
- 32) «consentimento» significa «consentimento» tal como definido no ponto 11 do artigo 4.º do Regulamento (UE) 2016/679;
- 33) «tribunal nacional» significa um tribunal de um Estado-Membro na acepção do artigo 267.º do TFUE.

CAPÍTULO II

GUARDIÕES DE ACESSO

Artigo 3

Nomeação de guardas de acesso

1. Uma empresa será designada como gatekeeper se:
 - a) tem grande influência no mercado interno;
 - b) fornece um serviço de plataforma básico que é uma importante porta de entrada para que os usuários profissionais alcancem os usuários finais e
 - c) tenha uma posição forte e duradoura em relação às suas operações, ou seja provável que alcance tal posição num futuro próximo.
2. Presume-se que uma empresa cumpre os respectivos requisitos estabelecidos no parágrafo 1:
 - (a) em relação à alínea a) do n.º 1, sempre que a empresa atinja um volume de negócios anual na União igual ou superior a 7 500 000 000 EUR em cada um dos últimos três exercícios financeiros, ou sempre que a sua capitalização bolsista média ou valor justo de mercado equivalente seja de, pelo menos, 75 000 000 000 EUR no último exercício financeiro, e preste o mesmo serviço essencial de plataforma em, pelo menos, três Estados-Membros;
 - (b) em relação à alínea b) do n.º 1, quando fornece um serviço de plataforma essencial que, no último exercício financeiro, teve pelo menos 45 milhões de utilizadores finais ativos mensais estabelecidos ou localizados na União e pelo menos 10 000 utilizadores empresariais ativos anuais estabelecidos ou localizados na União, identificados e calculados de acordo com a metodologia e os indicadores estabelecidos no anexo;
 - (c) em relação ao parágrafo 1(c), quando os limiares estabelecidos na alínea b) deste parágrafo tiverem sido atingidos em cada um dos três últimos exercícios financeiros.
3. Sempre que uma empresa que fornece serviços essenciais de plataforma atingir todos os limiares estabelecidos no parágrafo 2, deve notificar a Comissão sem demora e, em qualquer caso, no prazo de dois meses a contar da data em que esses limiares foram atingidos e deve fornecer à Comissão as informações relevantes referidas no parágrafo 2. Essa notificação deve incluir as informações relevantes referidas no parágrafo 2 para cada um dos serviços essenciais de plataforma da empresa que atingir os limiares estabelecidos no parágrafo 2, alínea b). Sempre que um novo serviço de plataforma essencial fornecido por uma empresa que tenha sido anteriormente designada como controladora de acesso atinja os limiares estabelecidos nas alíneas b) e c) do n.º 2, a empresa deve notificar a Comissão no prazo de dois meses a contar da data em que esses limiares foram atingidos.

Caso a empresa que fornece o serviço de plataforma principal não cumpra o requisito de notificação à Comissão estabelecido no primeiro parágrafo deste parágrafo e não forneça, dentro do prazo estabelecido pela Comissão na solicitação de informações nos termos do artigo 21.º, todas as informações relevantes necessárias para que a Comissão designe a empresa em causa como controladora de acesso, em conformidade com o parágrafo 4.º deste artigo, a Comissão manterá o poder de designar essa empresa como controladora de acesso, com base nas informações à sua disposição.

Caso a empresa que fornece serviços básicos de plataforma cumpra o pedido de informações nos termos do segundo parágrafo do presente parágrafo ou caso as informações sejam fornecidas após o termo do período referido nesse parágrafo, a Comissão aplicará o procedimento estabelecido no parágrafo 4.

4. A Comissão deve designar como controlador de acesso, sem demora injustificada e no prazo máximo de 45 dias úteis após a receção das informações completas referidas no n.º 3, uma empresa que forneça serviços essenciais de plataforma que cumpra todos os limiares estabelecidos no n.º 2.

5. A empresa que presta serviços essenciais de plataforma pode apresentar, juntamente com a sua notificação, argumentos suficientemente fundamentados para demonstrar que, excepcionalmente, apesar de ter cumprido todos os limiares previstos no n.º 2, dadas as circunstâncias em que o serviço essencial de plataforma em causa opera, não cumpre os requisitos enumerados no n.º 1.

Caso a Comissão considere que os argumentos apresentados nos termos do primeiro parágrafo pela empresa que fornece serviços básicos de plataforma não estão suficientemente fundamentados porque não colocam manifestamente em causa as presunções estabelecidas no n.º 2 do presente artigo, pode rejeitar esses argumentos no prazo referido no n.º 4, sem aplicar o procedimento previsto no artigo 17.º, n.º 3.

Caso a empresa que fornece serviços básicos de plataforma apresente argumentos suficientemente fundamentados que ponham manifestamente em causa as presunções estabelecidas no n.º 2 do presente artigo, a Comissão pode, em derrogação do primeiro parágrafo do presente número, no prazo referido no n.º 4 do presente artigo, dar início ao procedimento previsto no artigo 17.º, n.º 3.

Se a Comissão verificar que a empresa que fornece serviços essenciais de plataforma não conseguiu demonstrar que os serviços essenciais de plataforma relevantes que fornece não cumprem os requisitos estabelecidos no n.º 1 do presente artigo, deve designar essa empresa como controladora de acesso, em conformidade com o procedimento estabelecido no artigo 17.º, n.º 3.

6. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 49.º, a fim de complementar o presente regulamento, especificando a metodologia para determinar se os limiares quantitativos estabelecidos no n.º 2 do presente artigo são cumpridos e para ajustar periodicamente essa metodologia à evolução do mercado e tecnológica, sempre que necessário.

7. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 49.º, para alterar o presente regulamento, atualizando a metodologia e a lista de indicadores constantes do anexo.

8. A Comissão designará como controlador de acesso, de acordo com o procedimento estabelecido no artigo 17.º, qualquer empresa que forneça serviços essenciais de plataforma que cumpra todos os requisitos do n.º 1 do presente artigo, mas que não cumpra todos os limiares estabelecidos no n.º 2 do presente artigo.

Para o efeito, a Comissão terá em conta alguns ou todos os seguintes elementos, na medida em que sejam relevantes para a empresa que fornece os principais serviços de plataforma em causa:

(a) a dimensão, incluindo o volume de negócios e a capitalização bolsista, as operações e a posição dessa empresa;

b) o número de usuários profissionais que utilizam o serviço básico da plataforma para alcançar os usuários finais e o número de usuários finais;

- (c) efeitos de rede e benefícios de dados, em particular em relação ao acesso da empresa a dados pessoais e não pessoais, à coleta de tais dados pela empresa ou às suas capacidades de análise;
- (d) quaisquer efeitos relacionados com a escala ou o âmbito de que a empresa beneficia, em especial no que diz respeito aos dados e, se for caso disso, às suas atividades fora da União;
- (e) o aprisionamento de empresas ou utilizadores finais, incluindo os custos de mudança de fornecedores e os preconceitos comportamentais que reduzem a capacidade das empresas e dos utilizadores finais de mudar de fornecedor ou de utilizar vários fornecedores para o mesmo serviço;
- f) uma estrutura de conglomerado ou integração vertical da empresa, permitindo-lhe, por exemplo, compensar ganhos e perdas entre atividades, combinar dados de diferentes fontes ou tirar partido da sua posição, ou
- g) outras características estruturais das empresas ou serviços.

Ao efetuar a sua avaliação nos termos do presente parágrafo, a Comissão terá em conta os desenvolvimentos previsíveis no que diz respeito aos elementos enumerados no segundo parágrafo, em especial qualquer concentração prevista que afete outra empresa que forneça serviços essenciais de plataforma ou qualquer outro serviço no setor digital ou que permita a recolha de dados.

Caso uma empresa que fornece um serviço de plataforma essencial que não cumpre os limiares quantitativos estabelecidos no parágrafo 2 não cumpra as medidas de investigação impostas pela Comissão de forma significativa e continue a não cumprir depois de ter sido convidada a cumprir dentro de um prazo razoável e a apresentar observações, a Comissão pode, com base nos dados à sua disposição, designar essa empresa como controladora.

9. Para cada empresa designada como controladora de acesso nos termos do parágrafo 4 ou do parágrafo 8, a Comissão deve listar na decisão de designação os serviços essenciais de plataforma relevantes fornecidos por essa empresa que sejam individualmente uma importante porta de entrada para os utilizadores empresariais chegarem aos utilizadores finais, conforme referido no parágrafo 1(b).

10. O controlador deverá cumprir as obrigações estabelecidas nos artigos 5.º, 6.º e 7.º no prazo de seis meses a contar da data em que um serviço de plataforma essencial for listado na decisão de designação nos termos do n.º 9 do presente artigo.

Artigo 4º

Revisão do status do gatekeeper

1. A Comissão pode, a pedido ou por sua própria iniciativa, reconsiderar, modificar ou revogar a qualquer momento uma decisão de designação tomada em conformidade com o artigo 3.º por um dos seguintes motivos:

- a) qualquer dos factos em que se baseou a decisão de designação tenha sofrido alterações substanciais;
- b) a decisão de designação foi baseada em informações incompletas, incorretas ou enganosas.

2. A Comissão deve periodicamente, e pelo menos a cada três anos, rever se os controladores de acesso continuam a cumprir os requisitos estabelecidos no artigo 3.º(1). Essa revisão deve também analisar se é adequado alterar a lista dos principais serviços de plataforma do controlador de acesso que são individualmente uma importante porta de entrada para os utilizadores empresariais chegarem aos utilizadores finais, conforme referido na alínea b) do artigo 3.º(1). Tal revisão não terá qualquer efeito suspensivo relativamente às obrigações do guardião.

A Comissão também examinará, pelo menos anualmente, se as novas empresas que prestam serviços básicos de plataforma cumprem esses requisitos.

A Comissão adotará uma decisão que confirme, altere ou revogue a decisão de designação sempre que considerar, com base nas revisões efetuadas nos termos do primeiro parágrafo, que os factos em que se baseou a designação das empresas que prestam serviços essenciais de plataforma como controladores de acesso foram alterados.

3. A Comissão publicará e atualizará uma lista de controladores de acesso e a lista de serviços essenciais de plataforma em relação aos quais os controladores de acesso devem cumprir as obrigações estabelecidas no Capítulo III de forma contínua.

CAPÍTULO III

PRÁTICAS DE GATEKEEPER QUE LIMITAM A DISPUTABILIDADE OU SÃO INJUSTAS

Artigo 5º

Obrigações dos guardiões

1. O controlador deve cumprir todas as obrigações estabelecidas neste artigo para cada um dos seus principais serviços de plataforma listados na decisão de designação nos termos do artigo 3.º(9).

2. O porteiro deve abster-se de:

- a) processar, com a finalidade de fornecer serviços de publicidade online, os dados pessoais de usuários finais que utilizam serviços de terceiros que fazem uso dos principais serviços da plataforma do Gatekeeper;
- b) combinar dados pessoais dos serviços principais da plataforma relevantes com dados pessoais de quaisquer serviços principais adicionais da plataforma ou quaisquer outros serviços fornecidos pelo gatekeeper ou com dados pessoais de serviços de terceiros;
- c) cruzar dados pessoais do serviço de plataforma principal relevante com outros serviços fornecidos separadamente pelo gatekeeper, incluindo outros serviços de plataforma principal, e vice-versa; e
- d) registrar usuários finais em outros serviços de gatekeeper para combinar dados pessoais;

a menos que o utilizador final tenha sido apresentado a essa opção específica e tenha dado o seu consentimento na aceção do artigo 4.º, ponto 11, e do artigo 7.º do Regulamento (UE) 2016/679.

Caso o utilizador final tenha recusado ou retirado o consentimento dado para os fins do primeiro parágrafo, o controlador não poderá solicitar o consentimento para o mesmo fim mais de uma vez no período de um ano.

A presente secção não prejudica a possibilidade de o controlador de acesso invocar o artigo 6.º, n.º 1, alíneas c), d) e e), do Regulamento (UE) 2016/679, quando aplicável.

3. O gatekeeper deve abster-se de aplicar obrigações que impeçam os utilizadores profissionais de oferecer os mesmos produtos ou serviços aos utilizadores finais através de serviços de intermediação online de terceiros ou do seu próprio canal de vendas online direto a preços ou condições diferentes daqueles oferecidos através dos serviços de intermediação online do gatekeeper.

4. O gatekeeper deve permitir que os usuários profissionais, gratuitamente, comuniquem e promovam ofertas, em particular com condições diferenciadas, entre os usuários finais adquiridos por meio de seu serviço básico de plataforma ou outros canais e concluam contratos com esses usuários finais, independentemente de, para essa finalidade, utilizarem os serviços básicos de plataforma do gatekeeper.

5. O gatekeeper deverá permitir que os usuários finais, por meio de seus principais serviços de plataforma, acessem e usem conteúdo, assinaturas, recursos ou outros itens por meio de aplicativos de computador de um usuário empresarial, inclusive quando tais usuários finais tiverem adquirido esses itens por meio do usuário empresarial relevante sem usar os principais serviços de plataforma do gatekeeper.

6. O controlador não deve, direta ou indiretamente, impedir ou limitar os usuários empresariais ou usuários finais de apresentar reclamações perante qualquer autoridade pública relevante, incluindo tribunais nacionais, alegando não conformidade do controlador com a legislação da União ou nacional relevante em relação a qualquer prática do controlador. Isto não prejudica o direito dos utilizadores profissionais e dos gatekeepers de estabelecerem nos seus contratos as condições de utilização dos mecanismos legais para o processamento de reclamações.

7. O gatekeeper não deve exigir que os usuários finais utilizem um serviço de autenticação, mecanismo de navegador da web ou serviço de pagamento ou serviços técnicos desse gatekeeper que permitam o fornecimento de serviços de pagamento, como sistemas de pagamento para compras no aplicativo desse gatekeeper, como parte dos serviços fornecidos por usuários empresariais que utilizam os principais serviços de plataforma do gatekeeper; e, no caso de usuários empresariais, o gatekeeper não exigirá que eles usem e ofereçam esses serviços ou interoperem com eles.

8. O controlador não deve exigir que os utilizadores empresariais ou os utilizadores finais subscrevam ou se registem em quaisquer serviços de plataforma essenciais adicionais listados na decisão de designação nos termos do artigo 3.º(9) ou que atinjam os limiares definidos na alínea b) do artigo 3.º(2) como condição para poderem utilizar, aceder, registar-se ou subscrever quaisquer dos serviços de plataforma essenciais desse controlador listados nos termos desse artigo.

9. O Gatekeeper fornecerá a cada anunciante a quem fornece serviços de publicidade online, ou a terceiros autorizados pelos anunciantes, mediante solicitação do anunciante, informações diárias e gratuitas sobre cada anúncio do anunciante, em relação a:

- (a) o preço e as comissões pagas por esse anunciante, incluindo todas as deduções e sobretaxas, por cada um dos serviços de publicidade online relevantes fornecidos pelo controlador;
- b) a remuneração recebida pelo editor com o seu consentimento, incluindo todas as deduções e sobretaxas, e
- c) as medidas a partir das quais são calculados cada um dos preços, comissões e remunerações.

Caso um editor não consinta na partilha de informações relativas à remuneração recebida, conforme referido na alínea b) do primeiro parágrafo, o controlador deverá fornecer a cada anunciante, gratuitamente, informações relativas à remuneração média diária recebida por esse editor, incluindo todas as deduções e sobretaxas, para os anúncios relevantes.

10. O Gatekeeper fornecerá a cada editor para o qual fornece serviços de publicidade on-line, ou a terceiros autorizados pelos editores, mediante solicitação do editor, informações diárias e gratuitas sobre cada anúncio que apareça no inventário do editor, relacionadas a:

- (a) a remuneração recebida e as comissões pagas pelo editor, incluindo todas as deduções e sobretaxas, por cada um dos serviços de publicidade online relevantes fornecidos pelo controlador;
- b) o preço pago pelo anunciante com o seu consentimento, incluindo todas as deduções e sobretaxas, e
- c) a métrica a partir da qual cada um dos preços e remunerações são calculados.

Caso um anunciante não consinta com o compartilhamento de informações, o gatekeeper fornecerá a cada editor, gratuitamente, informações sobre o preço médio diário pago por esse anunciante, incluindo todas as deduções e sobretaxas, pelos anúncios relevantes.

Artigo 6º

Obrigações dos controladores de acesso que podem ser especificadas de forma mais aprofundada no artigo 8.º

1. O controlador deve cumprir todas as obrigações estabelecidas neste artigo para cada um dos seus principais serviços de plataforma listados na decisão de designação nos termos do artigo 3.º(9).

2. O Gatekeeper não deverá usar, em competição com Usuários Comerciais, quaisquer dados não acessíveis publicamente gerados ou fornecidos por tais Usuários Comerciais no contexto de seu uso dos Serviços Principais da Plataforma relevantes ou serviços fornecidos em conjunto com os Serviços Principais da Plataforma relevantes, ou em suporte a tais serviços, incluindo dados gerados ou fornecidos por clientes de tais Usuários Comerciais.

Para os fins do primeiro parágrafo, os dados não acessíveis ao público devem incluir todos os dados agregados e desagregados gerados por usuários comerciais que podem ser inferidos ou coletados por meio das atividades comerciais dos usuários comerciais ou de seus usuários finais, incluindo dados de clique, pesquisa, visualização e voz, nos serviços de plataforma principais relevantes ou em serviços fornecidos em conjunto com, ou em suporte aos, serviços de plataforma principais do gatekeeper relevante.

3. O gatekeeper deve permitir e habilitar tecnicamente os usuários finais a desinstalar facilmente qualquer aplicativo de software do sistema operacional do gatekeeper, sem prejuízo da possibilidade de o gatekeeper restringir a desinstalação de aplicativos de software pré-instalados que sejam essenciais para a operação do sistema operacional ou do dispositivo e que, do ponto de vista técnico, não possam ser oferecidos de forma autônoma por terceiros.

O Gatekeeper permitirá e habilitará tecnicamente os usuários finais a modificar facilmente as configurações padrão do sistema operacional, do assistente virtual e do navegador da web do Gatekeeper ao direcionar ou direcionar os usuários finais para produtos ou serviços oferecidos pelo Gatekeeper. Isso inclui pedir aos usuários finais, no momento do primeiro uso de um mecanismo de busca on-line, assistente virtual ou navegador da web do controlador listado na decisão de designação de acordo com o Artigo 3(9), que escolham, de uma lista dos principais provedores de serviços disponíveis, o mecanismo de busca on-line, assistente virtual ou navegador para o qual o sistema operacional do controlador direciona ou guia os usuários por padrão, e o mecanismo de busca on-line para o qual o assistente virtual e o navegador do controlador direcionam ou guiam os usuários por padrão.

4. O gatekeeper deverá permitir e viabilizar tecnicamente a instalação e o uso efetivo de aplicativos de computador de terceiros ou lojas de aplicativos de computador que utilizem ou interoperem com seu sistema operacional, e deverá permitir o acesso a tais aplicativos de computador ou lojas de aplicativos de computador por meios diferentes dos serviços básicos de plataforma relevantes desse gatekeeper. O gatekeeper não impedirá, quando aplicável, que aplicativos de computador de terceiros ou lojas de aplicativos de computador baixados solicitem que os usuários finais decidam se desejam definir tais aplicativos de computador ou lojas de aplicativos de computador baixados como a opção padrão. O gatekeeper permitirá tecnicamente que os usuários finais que escolherem definir o aplicativo de computador baixado ou a loja de aplicativos como a opção padrão façam a alteração facilmente.

Na medida em que estas sejam estritamente necessárias e proporcionais, o controlador não será impedido de tomar medidas para garantir que as aplicações informáticas ou as lojas de aplicações informáticas de terceiros não comprometam a integridade do sistema operacional fornecido pelo gatekeeper, desde que tais medidas não excedam o estritamente necessário e proporcional e sejam devidamente justificadas pelo gatekeeper.

Além disso, na medida em que sejam estritamente necessárias e proporcionais, o guardião não será impedido de aplicar medidas e configurações diferentes das configurações padrão que permitam aos usuários finais proteger efetivamente a segurança em relação a aplicativos de computador de terceiros ou lojas de aplicativos de computador, desde que tais medidas e configurações diferentes das configurações padrão sejam devidamente justificadas pelo guardião.

5. O gatekeeper não tratará, nem na classificação nem em funções relacionadas de indexação e rastreamento, os serviços e produtos oferecidos pelo próprio gatekeeper de forma mais favorável do que serviços ou produtos semelhantes de terceiros. O guardião deverá aplicar condições transparentes, justas e não discriminatórias a tal classificação.

6. O gatekeeper não deve restringir, técnica ou de outra forma, a capacidade dos usuários finais de alternar e assinar diferentes aplicativos e serviços de computador acessíveis por meio dos principais serviços de plataforma do gatekeeper, inclusive no que diz respeito à escolha de serviços de acesso à Internet para usuários finais.

7. O gatekeeper de acesso permitirá que os prestadores de serviços e fornecedores de ferramentas interoperem livre e eficazmente com as mesmas funções de ferramentas e programas acessíveis ou controláveis através do sistema operacional ou assistente virtual listado na decisão de designação de acordo com o Artigo 3(9) que são disponibilizados para os serviços ou ferramentas fornecidos ou fornecido pelo porteiro; e também permitirá o acesso a essas funções para fins de interoperabilidade. O gatekeeper também permitirá aos usuários profissionais e provedores alternativos de serviços fornecidos em conjunto com os serviços da plataforma principal, ou em suporte a tais serviços, interoperabilidade livre e efetiva com as mesmas funções do sistema operacional, ferramentas ou o software, e acesso a tais recursos para fins de interoperabilidade, independentemente de tais recursos fazerem parte do sistema operacional, estarem disponíveis para esse gatekeeper ou serem usados por esse gatekeeper no fornecimento de tais serviços.

O controlador não pode ser impedido de tomar medidas estritamente necessárias e proporcionais para garantir que a interoperabilidade não comprometa a integridade das funções do sistema operativo, do assistente virtual, de ferramentas ou programas fornecidas pelo porteiro, desde que devidamente justificadas essas medidas.

8. O Gatekeeper fornecerá aos anunciantes e editores, bem como a terceiros autorizados pelos anunciantes e editores, mediante solicitação e gratuitamente, acesso às ferramentas de medição de desempenho do Gatekeeper e aos dados necessários para que anunciantes e editores conduzam sua própria verificação independente do inventário de publicidade, incluindo dados agregados e desagregados. Esses dados serão fornecidos de uma maneira que permita que anunciantes e editores usem suas próprias ferramentas de verificação e medição para avaliar o desempenho dos principais serviços de plataforma fornecidos pelo gatekeeper.

9. O gatekeeper deve fornecer aos usuários finais e terceiros autorizados por um usuário final, mediante solicitação e gratuitamente, portabilidade efetiva dos dados fornecidos pelo usuário final ou gerados pela atividade do usuário final no contexto do uso do serviço de plataforma principal relevante, por exemplo, fornecendo ferramentas gratuitas para facilitar o exercício efetivo dessa portabilidade de dados, bem como acesso contínuo e em tempo real a esses dados.

10. O Gatekeeper fornecerá aos Usuários Profissionais e terceiros autorizados por um Usuário Profissional, mediante solicitação e gratuitamente, acesso efetivo, de qualidade, contínuo e em tempo real a dados agregados ou desagregados, e ao uso de tais dados, incluindo dados pessoais, fornecidos ou gerados no contexto do uso dos Serviços da Plataforma Principal ou serviços fornecidos em conjunto com ou em suporte aos Serviços da Plataforma Principal relevantes por tais Usuários Profissionais e usuários finais que usam produtos ou serviços fornecidos por tais Usuários Profissionais. Em relação aos dados pessoais, o gatekeeper fornecerá tal acesso ou uso de dados pessoais somente quando tais dados estiverem diretamente relacionados ao uso dos produtos ou serviços oferecidos pelo usuário comercial relevante por meio do serviço de plataforma principal relevante, e quando o usuário final optar por tal compartilhamento dando seu consentimento.

11. O gatekeeper deverá fornecer aos provedores terceirizados de mecanismos de busca on-line, mediante solicitação, acesso em termos justos, razoáveis e não discriminatórios a dados sobre classificações, consultas, cliques e visualizações em relação a pesquisas gratuitas e pagas geradas por usuários finais em seus mecanismos de busca on-line. Quaisquer consultas, cliques e visualizações de dados que sejam dados pessoais serão anonimizados.

12. O controlador aplicará aos utilizadores empresariais condições gerais de acesso justas, razoáveis e não discriminatórias às suas lojas de aplicações informáticas, motores de busca online e serviços de redes sociais online enumerados na decisão de designação, nos termos do artigo 3.º(9).

Para esse fim, o gatekeeper publicará condições gerais de acesso, incluindo um mecanismo alternativo de resolução de disputas.

A Comissão avaliará se as condições gerais de acesso publicadas cumprem as disposições da presente secção.

13. O gatekeeper não deve estabelecer condições gerais para a rescisão da prestação de um serviço básico de plataforma que sejam desproporcionais. O guardião deve garantir que as condições de rescisão possam ser exercidas sem dificuldades indevidas.

Artigo 7

Obrigações dos gatekeepers quanto à interoperabilidade dos serviços de comunicações interpessoal independente de numeração

1. Sempre que um controlador de acesso fornecer serviços de comunicações interpessoais independentes de número, conforme enumerados na decisão de designação nos termos do artigo 3.º(9), deverá tornar as funcionalidades essenciais dos seus serviços de comunicações interpessoais independentes de número interoperáveis com os serviços de comunicações interpessoais independentes de número de outro fornecedor que ofereça ou pretenda oferecer tais serviços na União, fornecendo as interfaces técnicas necessárias ou soluções semelhantes que facilitem a interoperabilidade, mediante pedido e gratuitamente.

2. O controlador de acesso deve garantir, pelo menos, a interoperabilidade das seguintes funcionalidades básicas referidas no n.º 1, quando ele próprio fornece essas funcionalidades aos seus próprios utilizadores finais:

(a) após a listagem da decisão de designação nos termos do artigo 3.º(9):

- i) mensagens de texto de ponta a ponta entre dois utilizadores finais individuais,
- ii) a troca de imagens, mensagens de voz, vídeos e outros arquivos anexados à comunicação de ponta a ponta entre dois utilizadores finais individuais;

b) no prazo de dois anos a contar da nomeação:

- i) mensagens de texto de ponta a ponta entre grupos de utilizadores finais individuais,
- ii) a troca de imagens, mensagens de voz, vídeos e outros arquivos anexados à comunicação de ponta a ponta entre um bate-papo em grupo e um utilizador final individual;

c) no prazo de quatro anos a contar da nomeação:

- i) chamadas de voz de ponta a ponta entre dois utilizadores finais individuais,
- ii) videochamadas de ponta a ponta entre dois utilizadores finais individuais,
- iii) chamadas de voz de ponta a ponta entre um chat em grupo e um utilizador final individual,
- iv) videochamadas de ponta a ponta entre um bate-papo em grupo e um utilizador final individual.

3. O nível de segurança, incluindo criptografia de ponta a ponta, se aplicável, fornecido pelo gatekeeper aos seus próprios utilizadores finais deve ser mantido em todos os serviços interoperáveis.

4. O gatekeeper deve publicar uma oferta de referência estabelecendo os detalhes técnicos e os princípios e condições gerais de interoperabilidade com seus serviços de comunicações interpessoais independentes de número, incluindo os detalhes necessários sobre o nível de segurança e criptografia de ponta a ponta. O controlador deverá publicar essa oferta de referência dentro do prazo especificado no Artigo 3, parágrafo 10, e atualizá-la quando necessário.

5. Após a publicação da oferta de referência nos termos do parágrafo 4, qualquer fornecedor de serviços de comunicações interpessoais independentes de número que ofereça ou pretenda oferecer tais serviços na União pode solicitar interoperabilidade com os serviços de comunicações interpessoais independentes de número fornecidos pelo controlador. Tal solicitação pode incluir algumas ou todas as funcionalidades básicas listadas na seção 2. O gatekeeper processará qualquer solicitação razoável de interoperabilidade dentro de três meses após o recebimento, tornando operacionais as funcionalidades básicas solicitadas.

6. Excepcionalmente, a Comissão pode, mediante solicitação fundamentada do controlador de acesso, estender os períodos de conformidade estabelecidos nos parágrafos 2 ou 5, quando o controlador de acesso demonstrar que tal extensão é necessária para garantir a interoperabilidade efetiva e para manter o nível de segurança exigido, incluindo criptografia de ponta a ponta, quando aplicável.

7. Os utilizadores finais dos serviços de comunicações interpessoais independentes de número do gatekeeper e o fornecedor de serviços de comunicações interpessoais independentes de número requerente permanecerão livres para decidir se pretendem utilizar as funcionalidades básicas interoperáveis que podem ser fornecidas pelo gatekeeper nos termos do parágrafo 1.

8. O gatekeeper deverá coletar e trocar com o provedor de serviços de comunicações interpessoais independentes de número que envia uma solicitação de interoperabilidade apenas os dados pessoais dos usuários finais que sejam estritamente necessários para fornecer interoperabilidade efetiva. Essa coleta e compartilhamento de dados pessoais de usuários finais estarão em total conformidade com o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE.

9. O gatekeeper não será impedido de tomar medidas para garantir que terceiros provedores de serviços de comunicações interpessoais independentes de número que solicitem interoperabilidade não coloquem em risco a integração, a segurança e a confidencialidade de seus serviços, desde que tais medidas sejam estritamente necessárias e proporcionais e sejam devidamente justificadas pelo gatekeeper.

Artigo 8

Cumprimento das obrigações dos gatekeepers

1. O controlador deve garantir e demonstrar o cumprimento das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º do presente regulamento. As medidas aplicadas pelo controlador para garantir o cumprimento desses artigos devem ser eficazes para atingir os objetivos do presente regulamento e da obrigação correspondente. O controlador deve garantir que a aplicação de tais medidas esteja em conformidade com a legislação aplicável, em especial o Regulamento (UE) 2016/679, a Diretiva 2002/58/CE, a legislação sobre segurança cibernética, proteção do consumidor e segurança dos produtos, e os requisitos de acessibilidade.

2. A Comissão pode, por sua própria iniciativa ou a pedido de um controlador de acesso, nos termos do parágrafo 3 do presente artigo, iniciar um procedimento nos termos do artigo 20.º.

A Comissão pode adotar um ato de execução que especifique as medidas a implementar pelo controlador de acesso em causa para cumprir efetivamente as obrigações estabelecidas nos artigos 6.º e 7.º. Esse ato de execução deve ser adotado no prazo de seis meses a contar do início do procedimento previsto no artigo 20.º, em conformidade com o procedimento consultivo referido no artigo 50.º, n.º 2.

Ao iniciar um procedimento com base em motivos de evasão nos termos do artigo 13.º, tais medidas podem referir-se às obrigações estabelecidas nos artigos 5.º, 6.º e 7.º.

3. Um controlador de acesso pode solicitar à Comissão que participe de um procedimento para determinar se as medidas que o controlador de acesso pretende implementar ou implementou para garantir a conformidade com os artigos 6.º e 7.º são eficazes para atingir o objetivo da obrigação relevante nas circunstâncias específicas do controlador de acesso. A Comissão terá poder discricionário para decidir se participa ou não de tal procedimento, respeitando os princípios de igualdade de tratamento, proporcionalidade e boa administração.

No seu pedido, o controlador deverá apresentar uma declaração fundamentada explicando as medidas que pretende implementar ou implementou. Além disso, o controlador deverá fornecer uma versão não confidencial da sua submissão fundamentada, que poderá ser partilhada com terceiros, em conformidade com o parágrafo 6.

4. Os parágrafos 2 e 3 do presente artigo não prejudicam os poderes conferidos à Comissão pelos artigos 29, 30 e 31.

5. Com vista à adoção da decisão prevista no n.º 2, a Comissão comunicará as suas conclusões preliminares ao controlador de acesso no prazo de três meses a contar do início do procedimento previsto no artigo 20.º. Nas conclusões preliminares, a Comissão explicará as medidas que considera que deve tomar ou que considera que o controlador de acesso em causa deve tomar para abordar eficazmente as conclusões preliminares.

6. A fim de permitir que terceiros interessados comentem efetivamente, ao comunicar suas conclusões preliminares ao controlador de acesso, nos termos do parágrafo 5, ou o mais rápido possível após comunicar essas conclusões, a Comissão publicará um resumo não confidencial do caso e das medidas que está considerando tomar ou considera que deveriam ser tomadas pelo controlador de acesso em questão. A Comissão fixará um prazo razoável para a apresentação dessas observações.

7. Ao especificar as medidas previstas no n.º 2, a Comissão deve assegurar que as medidas sejam eficazes na concretização dos objetivos do presente regulamento e da obrigação correspondente, e proporcionais às circunstâncias específicas do controlador de acesso e do serviço em causa.

8. Para efeitos de especificação das obrigações previstas no artigo 6.º(11) e (12), a Comissão deve também avaliar se as medidas planeadas ou implementadas garantem que não subsiste qualquer desequilíbrio entre os direitos e as obrigações dos utilizadores empresariais e que as medidas não conferem, por si só, uma vantagem ao controlador de acesso que seja desproporcional ao serviço prestado pelo controlador de acesso aos utilizadores empresariais.

9. No que se refere ao procedimento previsto no n.º 2, a Comissão pode, a pedido ou por sua própria iniciativa, decidir reabrir o procedimento quando:

- a) houve uma alteração significativa em qualquer dos factos em que a decisão se baseou, ou
- b) a decisão foi baseada em informações incompletas, incorretas ou enganosas, ou
- c) as medidas especificadas na decisão não são eficazes.

Artigo 9

Suspensão

1. Sempre que o controlador de acesso demonstrar, num pedido fundamentado, que o cumprimento de uma obrigação específica estabelecida nos artigos 5.º, 6.º ou 7.º para um serviço de plataforma essencial enumerado na decisão de designação nos termos do artigo 3.º, n.º 9, poderia, devido a circunstâncias excecionais fora do seu controlo, pôr em risco a viabilidade económica das suas operações na União, a Comissão pode adotar um ato de execução que estabeleça a sua decisão de suspender, a título excecional, no todo ou em parte, a obrigação específica referida nesse pedido fundamentado («a decisão de suspensão»). Nesse ato de execução, a Comissão justifica a sua decisão de suspensão indicando as circunstâncias excecionais que justificam a suspensão. Tal ação de execução será limitada à extensão e duração necessárias para lidar com tal ameaça à viabilidade do gatekeeper. A Comissão deve esforçar-se por adotar tal ato de execução sem demora e, o mais tardar, três meses após a receção de um pedido completo e fundamentado. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

2. Quando a suspensão for concedida nos termos do parágrafo 1, a Comissão deverá rever a sua decisão de suspensão anualmente, a menos que um período mais curto seja especificado na decisão. Após essa revisão, a Comissão levantará a suspensão total ou parcialmente ou decidirá que as condições estabelecidas no parágrafo 1 devem continuar a ser cumpridas.

3. Em casos de urgência e mediante solicitação fundamentada de um controlador de acesso, a Comissão pode suspender provisoriamente a aplicação de uma obrigação específica referida no parágrafo 1 para um ou mais serviços essenciais de plataforma individuais antes de adotar a decisão prevista naquele parágrafo. Tal solicitação pode ser apresentada e atendida a qualquer momento, aguardando a avaliação da Comissão, nos termos do parágrafo 1.

4. Ao analisar o pedido referido nos n.ºs 1 e 3, a Comissão terá em conta, em especial, o impacto do cumprimento da obrigação específica na viabilidade económica das operações do controlador de acesso na União e em terceiros, em especial as PME e os consumidores. A suspensão pode estar sujeita a condições e obrigações definidas pela Comissão para garantir um equilíbrio justo entre esses interesses e os objetivos do presente regulamento.

Artigo 10

Isenção por razões de saúde pública e segurança pública

1. Mediante pedido fundamentado de um controlador de acesso ou por sua própria iniciativa, a Comissão pode adotar um ato de execução que estabeleça a sua decisão de isentar esse controlador de acesso, no todo ou em parte, de uma obrigação específica estabelecida nos artigos 5.º, 6.º ou 7.º em relação a um serviço essencial de plataforma enumerado na decisão de designação nos termos do artigo 3.º, n.º 9, sempre que tal isenção seja justificada pelos motivos estabelecidos no n.º 3 do presente artigo («a decisão de isenção»). A Comissão adotará a decisão de isenção no prazo de três meses a contar da receção de um pedido completo e fundamentado e fornecerá uma declaração fundamentada explicando os motivos da isenção. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.
2. Quando for concedida uma isenção nos termos do parágrafo 1, a Comissão deverá rever a sua decisão de isenção quando o motivo da isenção deixar de existir ou, pelo menos, anualmente. Após essa revisão, a Comissão deverá levantar a isenção total ou parcialmente ou decidir que as condições estabelecidas no parágrafo 1 devem continuar a ser cumpridas.
3. A isenção prevista no n.º 1 só pode ser concedida por motivos de saúde pública ou de segurança pública.
4. Em casos de urgência e mediante pedido fundamentado de um controlador de acesso ou por sua própria iniciativa, a Comissão pode suspender provisoriamente a aplicação de uma obrigação específica referida no n.º 1 para um ou mais serviços essenciais de plataforma individuais antes de adotar a decisão prevista nesse número. Tal solicitação pode ser apresentada e atendida a qualquer momento, aguardando a avaliação da Comissão, nos termos do parágrafo 1.
5. Ao analisar o pedido referido nos n.ºs 1 e 4, a Comissão terá em conta, em especial, o impacto do cumprimento da obrigação específica pelos motivos estabelecidos no n.º 3, bem como as consequências para o controlador de acesso relevante e para terceiros. A Comissão pode sujeitar a suspensão a condições e obrigações para assegurar um equilíbrio justo entre os objetivos prosseguidos pelos motivos estabelecidos no n.º 3 e os objetivos do presente regulamento.

Artigo 11

Informação

1. No prazo de seis meses a contar da sua designação nos termos do artigo 3.º e em conformidade com o artigo 3.º(10), o controlador de acesso deve fornecer à Comissão um relatório descrevendo de forma detalhada e transparente as medidas que implementou para garantir o cumprimento das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º.
2. No prazo referido no n.º 1, o controlador de acesso deve publicar um resumo não confidencial desse relatório e fornecê-lo à Comissão.

O gatekeeper atualizará o relatório e o resumo não confidencial pelo menos uma vez por ano.

A Comissão disponibilizará um link para este resumo não confidencial no seu sítio Web.

Artigo 12

Atualização das obrigações dos gatekeepers

1. A Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 49.º para complementar o presente regulamento no que diz respeito às obrigações estabelecidas nos artigos 5.º e 6.º. Esses atos delegados devem basear-se numa investigação de mercado nos termos do artigo 19.º, que tenha identificado a necessidade de atualizar essas obrigações, a fim de abordar práticas que limitem a disputabilidade dos serviços essenciais de plataforma ou que sejam desleais da mesma forma que as práticas abrangidas pelas obrigações estabelecidas nos artigos 5.º e 6.º.

2. O âmbito de um ato delegado adotado nos termos do parágrafo 1 será limitado a:

- (a) alargar uma obrigação que apenas se aplica em relação a determinados serviços essenciais de plataforma a outros serviços essenciais de plataforma enumerados no artigo 2.º, ponto 2;
- b) estender uma obrigação que beneficia certos utilizadores profissionais ou utilizadores finais para que beneficie outros utilizadores profissionais ou utilizadores finais;
- (c) especificar o modo como os controladores de acesso devem cumprir as obrigações estabelecidas nos artigos 5.º e 6.º, a fim de garantir o cumprimento efetivo dessas obrigações;
- (d) estender uma obrigação que se aplica apenas em relação a determinados serviços prestados em conjunto com ou em apoio aos serviços essenciais da plataforma a outros serviços prestados em conjunto com ou em apoio aos serviços essenciais da plataforma;
- (e) estender uma obrigação que só se aplica em relação a certos tipos de dados a outros tipos de dados;
- f) introduzir novas condições quando uma obrigação impõe certas condições relativamente ao comportamento do controlador, ou
- g) aplicar uma obrigação que rege a relação entre vários serviços de plataforma central de gatekeeper à relação entre um serviço de plataforma central de gatekeeper e outros serviços de gatekeeper.

3. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 49.º, para alterar o presente regulamento no que diz respeito à lista de funcionalidades básicas referidas no artigo 7.º, n.º 2, adicionando ou removendo funcionalidades de serviços de comunicações interpessoais independentes do número.

Esses atos delegados devem basear-se numa investigação de mercado nos termos do artigo 19.º, que tenha identificado a necessidade de atualizar essas obrigações para abordar práticas que limitem a disputabilidade dos serviços essenciais da plataforma ou que sejam desleais da mesma forma que as práticas abrangidas pelas obrigações estabelecidas no artigo 7.º.

4. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 49.º, para complementar o presente regulamento no que diz respeito às obrigações estabelecidas no artigo 7.º, especificando a forma como essas obrigações devem ser cumpridas, a fim de assegurar a sua execução efetiva. Esses atos delegados devem basear-se em uma investigação de mercado nos termos do artigo 19, que determina a necessidade de atualizar essas obrigações para abordar práticas que limitam a disputabilidade dos serviços essenciais da plataforma ou que são desleais da mesma forma que as práticas referidas nas obrigações estabelecidas no artigo 7.º.

5. Uma prática referida nos n.os 1, 3 e 4 será considerada limitadora da contestabilidade dos serviços básicos de plataforma ou injusta quando:

- a) tal prática é realizada por gatekeepers e pode dificultar a inovação e limitar a escolha de usuários profissionais e usuários finais porque:
 - (i) afete ou ameace afetar a contestabilidade de um serviço de plataforma essencial ou de outros serviços do setor digital de forma duradoura devido à criação ou consolidação de barreiras à entrada de outras empresas ou ao seu desenvolvimento como fornecedores de um serviço de plataforma essencial ou de outros serviços do setor digital, ou
 - ii) impede que outros operadores tenham o mesmo acesso a uma entrada de chave que o gatekeeper, ou
- b) há um desequilíbrio entre os direitos e obrigações dos usuários profissionais e o gatekeeper obtém dos usuários profissionais uma vantagem desproporcional ao serviço que presta a esses usuários profissionais.

Artigo 13

Anti-evasão

1. Uma empresa que fornece serviços de plataforma essenciais não deve segmentar, dividir, subdividir, fragmentar ou separar serviços por meios contratuais, comerciais, técnicos ou outros, a fim de contornar os limites quantitativos estabelecidos no Artigo 3(2). Qualquer prática desse tipo por uma empresa não deve impedir a Comissão de designá-la como um gatekeeper nos termos do Artigo 3(4).

2. Sempre que a Comissão suspeitar que uma empresa que fornece serviços básicos de plataforma esteja envolvida em qualquer uma das práticas estabelecidas no parágrafo 1, poderá exigir que essa empresa forneça quaisquer informações que considere necessárias para determinar se a empresa em questão se envolveu em tal prática.

3. Os controladores de acesso devem assegurar que as obrigações estabelecidas nos artigos 5.º, 6.º e 7.º sejam cumpridas de forma plena e eficaz.

4. Os gatekeepers não devem adotar qualquer conduta que comprometa o cumprimento efetivo das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º, independentemente de tal conduta ser contratual, comercial, técnica ou de qualquer outra natureza, ou consistir na utilização de técnicas baseadas no comportamento ou na conceção de interfaces.

5. Quando for necessário o consentimento para a coleta, processamento, correspondência e compartilhamento de dados pessoais para garantir a conformidade com o presente regulamento, os controladores de acesso devem tomar as medidas adequadas para permitir que os usuários empresariais obtenham diretamente o consentimento necessário para seu processamento, quando tal consentimento for exigido pelo Regulamento (UE) 2016/679 ou pela Diretiva 2002/58/CE, ou para cumprir as regras e princípios de proteção de dados e privacidade da União de outras maneiras, por exemplo, fornecendo aos usuários empresariais dados adequadamente anonimizados, quando apropriado. Os gatekeepers não tornarão a obtenção desse consentimento do usuário comercial mais onerosa do que para seus próprios serviços.

6. Os gatekeepers não devem degradar as condições ou a qualidade de quaisquer serviços essenciais da plataforma fornecidos aos usuários empresariais ou usuários finais que se beneficiem dos direitos ou escolhas estabelecidos nos Artigos 5, 6 e 7, nem dificultar indevidamente o exercício desses direitos ou escolhas, inclusive oferecendo escolhas aos usuários finais de forma não neutra ou subvertendo a autonomia e a tomada de decisões ou escolhas dos usuários finais ou empresariais por meio da estrutura, design, função ou modo de operação da interface do usuário ou de seus componentes.

7. Sempre que os controladores de acesso contornarem ou tentarem contornar qualquer uma das obrigações estabelecidas nos artigos 5.º, 6.º ou 7.º da forma descrita nos n.ºs 4, 5 e 6 do presente artigo, a Comissão pode iniciar um procedimento nos termos do artigo 20.º e adotar um ato de execução nos termos do artigo 8.º, n.º 2, especificando as medidas a tomar pelos controladores de acesso.

8. O parágrafo 6 do presente artigo não prejudica os poderes conferidos à Comissão pelos artigos 29, 30 e 31.

Artigo 14

Obrigação de comunicar concentrações

1. Os controladores de acesso devem informar a Comissão de qualquer proposta de concentração na aceção do artigo 3.º do Regulamento (CE) n.º 1099/2008, qualquer 139/2004, quando as entidades resultantes da concentração ou a empresa resultante da concentração prestam serviços básicos de plataforma ou quaisquer outros serviços no setor digital ou permitem a coleta de dados, independentemente de serem notificáveis à Comissão nos termos desse Regulamento ou a uma autoridade nacional de concorrência competente nos termos das regras nacionais sobre concentrações.

Os controladores devem informar a Comissão de tal concentração antes da sua implementação e após a celebração do acordo, o anúncio do concurso público ou a aquisição de uma participação maioritária.

2. As informações fornecidas pelos controladores de acesso nos termos do n.º 1 devem descrever, pelo menos, as empresas afetadas pela concentração, o seu volume de negócios anual na União e a nível mundial, as suas áreas de atividade, incluindo atividades diretamente relacionadas com a concentração, e o valor da transação do contrato ou uma estimativa do mesmo, juntamente com um resumo da concentração, incluindo a sua natureza e justificação, e uma lista dos Estados-Membros afetados pela concentração.

As informações fornecidas pelos controladores de acesso devem também descrever, relativamente a qualquer serviço de plataforma essencial relevante, o seu volume de negócios anual na União, o número de utilizadores empresariais ativos anuais e o número de utilizadores finais ativos mensais, respetivamente.

3. Se, na sequência de qualquer concentração referida no n.º 1 do presente artigo, os serviços essenciais de plataforma adicionais atingirem individualmente os limiares estabelecidos no artigo 3.º, n.º 2, alínea b), o controlador de acesso em causa deverá informar a Comissão desse facto no prazo de dois meses a contar da implementação da concentração e deverá fornecer à Comissão as informações referidas no artigo 3.º, n.º 2.

4. A Comissão transmite às autoridades competentes dos Estados-Membros todas as informações recebidas nos termos do n.º 1 e publica anualmente a lista das aquisições de que foi informada pelos controladores de acesso nos termos desse número.

A Comissão levará em consideração os interesses legítimos das empresas na proteção de seus segredos comerciais.

5. As autoridades competentes dos Estados-Membros podem utilizar as informações recebidas nos termos do n.º 1 do presente artigo para solicitar à Comissão que examine a concentração em conformidade com o artigo 22.º do Regulamento (CE) n.º 1189/2008.^{qualquer139/2004.}

Artigo 15

Obrigações de auditoria

1. No prazo de seis meses a contar da sua designação nos termos do artigo 3.º, os gatekeepers devem apresentar à Comissão uma descrição auditada de forma independente das técnicas de definição de perfis de consumidores que aplicam nos seus principais serviços de plataforma listados na decisão de designação nos termos do artigo 3.º(9). A Comissão deve transmitir essa descrição auditada ao Comité Europeu para a Proteção de Dados.

2. A Comissão pode adotar um ato de execução, tal como referido na alínea g) do artigo 46.º, n.º 1, para desenvolver a metodologia e o procedimento de auditoria.

3. Os controladores devem tornar público um resumo da descrição auditada referida no parágrafo 1. Ao fazê-lo, eles devem ter o direito de considerar a necessidade de respeitar seus segredos comerciais. Os guardiões atualizarão a descrição e o resumo pelo menos uma vez por ano.

CAPÍTULO IV

PESQUISA DE MERCADO

Artigo 16

Abertura de investigação de mercado

1. Sempre que a Comissão pretenda realizar uma investigação de mercado com vista a possíveis decisões ao abrigo dos artigos 17.º, 18.º e 19.º, deve adotar uma decisão para iniciar uma investigação de mercado.

2. Não obstante o disposto no n.º 1, a Comissão pode exercer os seus poderes de investigação ao abrigo do presente regulamento antes de iniciar uma investigação de mercado nos termos desse número.

3. A decisão a que se refere o n.º 1 deve especificar:

- a) a data de abertura da investigação de mercado;
- b) a descrição do problema a que se refere a pesquisa de mercado;
- c) a finalidade da pesquisa de mercado.

4. A Comissão pode reabrir uma investigação de mercado que tenha sido concluída quando:

- (a) tenha ocorrido uma alteração significativa em qualquer dos factos em que se baseia qualquer decisão tomada ao abrigo dos artigos 17.º, 18.º ou 19.º, ou
- (b) a decisão tomada nos termos dos artigos 17.º, 18.º ou 19.º se basear em informações incompletas, incorrectas ou enganosas.

5. A Comissão pode solicitar a uma ou mais autoridades nacionais competentes que a auxiliem na sua investigação de mercado.

Artigo 17

Pesquisa de mercado para designar gatekeepers

1. A Comissão pode realizar uma investigação de mercado com a finalidade de examinar se uma empresa que fornece serviços essenciais de plataforma deve ser designada como um gatekeeper nos termos do Artigo 3(8) ou para determinar quais serviços essenciais de plataforma devem ser listados na decisão de designação nos termos do Artigo 3(9). A Comissão deve esforçar-se por concluir a sua investigação de mercado no prazo de 12 meses a contar da data referida na alínea a) do Artigo 16(3). Para concluir sua investigação de mercado, a Comissão adotará uma decisão por meio de um ato de execução. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

2. Ao realizar uma investigação de mercado nos termos do n.º 1 do presente artigo, a Comissão deve esforçar-se por comunicar as suas conclusões preliminares à empresa que fornece serviços essenciais de plataforma em causa no prazo de seis meses a contar da data referida na alínea a) do artigo 16.º(3). Nas suas conclusões preliminares, a Comissão deve explicar se considera adequado, a título provisório, designar uma empresa controladora de acesso em conformidade com o artigo 3.º, n.º 8, e listar os serviços essenciais de plataforma relevantes em conformidade com o artigo 3.º, n.º 9.

3. Sempre que a empresa que fornece serviços essenciais de plataforma cumprir os limiares estabelecidos no artigo 3.º, n.º 2, mas tiver apresentado argumentos suficientemente fundamentados, em conformidade com o artigo 3.º, n.º 5, que tenham manifestamente posto em causa a presunção prevista no artigo 3.º, n.º 2, a Comissão deve esforçar-se por concluir a investigação de mercado no prazo de cinco meses a contar da data referida no artigo 16.º, n.º 3, alínea a).

Nesse caso, a Comissão deve esforçar-se por comunicar as suas conclusões preliminares, nos termos do n.º 2 do presente artigo, à empresa em causa no prazo de três meses a contar da data referida no artigo 16.º, n.º 3, alínea a).

4. Quando a Comissão, nos termos do artigo 3.º(8), designar como controlador de acesso uma empresa que fornece serviços básicos de plataforma e que ainda não goza de uma posição operacional forte e duradoura, mas que se espera que venha a gozar dessa posição num futuro próximo, pode declarar aplicáveis a esse controlador de acesso apenas uma ou mais das obrigações estabelecidas no artigo 5.º(3) a (6) e no artigo 6.º(4), (7), (9), (10) e (13), conforme especificado na decisão de designação. A Comissão só declarará aplicáveis as obrigações que sejam adequadas e necessárias para impedir que o controlador em causa obtenha, por meios desleais, uma posição forte e duradoura nas suas operações. A Comissão analisará essa designação de acordo com o procedimento estabelecido no artigo 4.º.

Artigo 18

Pesquisa de mercado sobre não conformidade sistemática

1. A Comissão pode realizar uma investigação de mercado para verificar se um controlador de acesso se envolveu em incumprimento sistemático. A Comissão concluirá essa investigação de mercado no prazo de doze meses a contar da data referida no artigo 16.º, n.º 3, alínea a). A Comissão adotará, por meio de um ato de execução, a decisão de encerrar a investigação de mercado. Caso a investigação de mercado revele que um controlador de acesso não cumpriu sistematicamente uma ou mais das obrigações estabelecidas nos artigos 5.º, 6.º ou 7.º e manteve, reforçou ou alargou a sua posição de controlador de acesso em relação aos requisitos estabelecidos no artigo 3.º, n.º 1, a Comissão pode adotar um ato de execução que imponha a esse controlador de acesso quaisquer medidas corretivas comportamentais ou estruturais que sejam proporcionais e necessárias para garantir o cumprimento efetivo do presente regulamento. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

2. A medida corretiva imposta nos termos do parágrafo 1 do presente artigo, na medida em que seja proporcional e necessária para manter ou restaurar a equidade e a contestabilidade quando estas tenham sido afetadas por uma não conformidade sistemática, pode incluir uma proibição, por um período limitado, de o controlador de acesso participar numa concentração na aceção do artigo 3.º do Regulamento (CE) n.º 1079/2008, qualquer 139/2004 no que diz respeito aos serviços básicos de plataforma, outros serviços prestados no setor digital ou serviços que permitam a recolha de dados que tenham sido afetados por incumprimento sistemático.

3. Considera-se que um controlador de acesso cometeu um incumprimento sistemático das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º quando a Comissão tiver adotado pelo menos três decisões de incumprimento nos termos do artigo 29.º contra o controlador de acesso em causa em relação a qualquer um dos seus principais serviços de plataforma nos oito anos anteriores à adoção da decisão de abertura de uma investigação de mercado com vista à possível adoção de uma decisão nos termos do presente artigo.

4. A Comissão comunicará as suas conclusões preliminares ao controlador de acesso em causa no prazo de seis meses a contar da data referida na alínea a) do artigo 16.º(3). Nas suas conclusões preliminares, a Comissão explicará se considera, numa base preliminar, que as condições do n.º 1 do presente artigo estão cumpridas e que medidas corretivas considera, numa base preliminar, necessárias e proporcionais.

5. A fim de permitir que terceiros interessados comentem de forma eficaz, a Comissão deverá, ao mesmo tempo em que comunicar as suas conclusões preliminares sobre o controlador de acesso, nos termos do parágrafo 4, ou o mais rapidamente possível após comunicá-las, publicar um resumo não confidencial do caso e de quaisquer medidas corretivas que esteja a considerar. A Comissão fixará um prazo razoável para a apresentação dessas observações.

6. Quando a Comissão adotar uma decisão nos termos do parágrafo 1 do presente artigo, tornando vinculativos os compromissos oferecidos pelo controlador de acesso nos termos do artigo 25, ela publicará um resumo não confidencial do caso e o conteúdo principal desses compromissos. Terceiros interessados podem apresentar suas observações dentro de um prazo razoável a ser fixado pela Comissão.

7. Enquanto a investigação de mercado estiver a ser realizada, a Comissão pode prolongar a sua duração sempre que tal prolongamento seja justificado por razões objetivas e seja proporcional. A prorrogação pode aplicar-se ao prazo dentro do qual a Comissão deve formular as suas conclusões preliminares ou ao prazo para a adoção da decisão final. A duração total de qualquer extensão ou extensões nos termos deste parágrafo não excederá seis meses.

8. A fim de garantir que o controlador cumpra efetivamente as obrigações estabelecidas nos artigos 5.º, 6.º e 7.º, a Comissão deve rever periodicamente as medidas corretivas que impõe em conformidade com os n.ºs 1 e 2 do presente artigo. A Comissão terá o poder de modificar tais medidas corretivas se, após uma nova investigação de mercado, concluir que elas não são eficazes.

Artigo 19

Pesquisa de mercado sobre novos serviços e novas práticas

1. A Comissão pode realizar uma investigação de mercado com vista a analisar se um ou mais serviços do setor digital devem ser adicionados à lista de serviços essenciais de plataforma estabelecida no artigo 2.º, n.º 2, ou com vista a identificar práticas que limitem a disputabilidade dos serviços essenciais de plataforma ou que sejam desleais e não sejam eficazmente abordadas pelo presente regulamento. No seu exame, a Comissão terá em conta as conclusões relevantes dos procedimentos conduzidos ao abrigo dos artigos 101.º e 102.º do TFUE em relação aos mercados digitais, bem como quaisquer outras circunstâncias relevantes.

2. Ao realizar uma investigação de mercado nos termos do parágrafo 1, a Comissão pode consultar terceiros, incluindo utilizadores profissionais e utilizadores finais de serviços do setor digital sob investigação e utilizadores profissionais e utilizadores finais sujeitos a práticas sob investigação.

3. A Comissão publicará as suas conclusões num relatório no prazo de dezoito meses a contar da data referida no artigo 16.º, n.º 3, alínea a).

Este relatório será apresentado ao Parlamento Europeu e ao Conselho e, quando adequado, será acompanhado de:

- (a) uma proposta legislativa para alterar o presente regulamento, a fim de incluir serviços adicionais do setor digital na lista de serviços essenciais de plataforma estabelecida no artigo 2.º, n.º 2, ou para incluir novas obrigações no Capítulo III, ou
- (b) um projeto de ato delegado que complemente o presente regulamento no que diz respeito às obrigações estabelecidas nos artigos 5.º e 6.º, ou um projeto de ato delegado que altere ou complemente o presente regulamento no que diz respeito às obrigações previstas no artigo 7.º, tal como previsto no artigo 12.º.

Se for caso disso, a proposta legislativa de alteração do presente regulamento nos termos da alínea a) do segundo parágrafo pode também propor a supressão de serviços da lista de serviços essenciais de plataforma estabelecida no artigo 2.º, n.º 2, ou a supressão de obrigações existentes nos termos dos artigos 5.º, 6.º ou 7.º.

CAPÍTULO V

HABILIDADES DE PESQUISA, EXECUÇÃO E SUPERVISÃO

Artigo 20

Início do processo

1. Sempre que a Comissão pretenda dar início a um procedimento com vista à possível adoção de decisões nos termos dos artigos 8.º, 29.º e 30.º, adotará uma decisão de início de procedimento.

2. Não obstante o disposto no n.º 1, a Comissão pode exercer os seus poderes de investigação ao abrigo do presente regulamento antes de iniciar um procedimento ao abrigo desse número.

Artigo 21

Pedidos de informação

1. Para desempenhar as suas funções ao abrigo do presente regulamento, a Comissão pode, mediante simples pedido ou por decisão, exigir que as empresas e associações de empresas forneçam todas as informações necessárias. A Comissão poderá ainda, por meio de simples requerimento ou decisão, solicitar acesso a quaisquer dados ou algoritmos das empresas e informações sobre os testes, bem como solicitar explicações sobre os mesmos.

2. Ao enviar um pedido simples de informação a uma empresa ou associação de empresas, a Comissão deve indicar a base jurídica e a finalidade do pedido, especificar quais as informações necessárias e fixar o prazo dentro do qual as informações devem ser fornecidas, bem como quaisquer sanções previstas no artigo 30.º aplicáveis à prestação de informações ou explicações incompletas, incorretas ou enganosas.

3. Sempre que a Comissão, por meio de uma decisão, exija que empresas e associações de empresas forneçam informações, deverá indicar a finalidade do pedido, especificar as informações necessárias e fixar o prazo dentro do qual as informações devem ser fornecidas. Quando a Comissão exigir que as empresas forneçam acesso a quaisquer dados, algoritmos e informações sobre testes, ela indicará a finalidade da solicitação e definirá o prazo dentro do qual ela deve ser fornecida. Deverá também indicar as sanções previstas no artigo 30.º e indicar ou impor as coimas previstas no artigo 31.º. Deverá também indicar o direito de a decisão ser sujeita a revisão pelo Tribunal de Justiça.

4. As empresas ou associações de empresas ou os seus representantes devem fornecer as informações solicitadas em nome da empresa ou associação de empresas em causa. Advogados devidamente autorizados podem fornecer informações em nome de seus clientes. Este último permanecerá totalmente responsável se as informações fornecidas estiverem incompletas, incorretas ou enganosas.

5. A pedido da Comissão, as autoridades competentes dos Estados-Membros devem fornecer-lhe todas as informações na sua posse necessárias ao desempenho das tarefas que lhe são conferidas pelo presente regulamento.

Artigo 22

Competência na condução de entrevistas e na tomada de depoimentos

1. Para desempenhar as suas funções ao abrigo do presente regulamento, a Comissão pode entrevistar qualquer pessoa singular ou coletiva que consinta em ser entrevistada, para efeitos de recolha de informações relacionadas com o objeto de uma investigação. A Comissão terá o poder de gravar tais entrevistas por quaisquer meios técnicos.

2. Sempre que uma entrevista nos termos do n.º 1 do presente artigo tiver lugar nas instalações de uma empresa, a Comissão deve informar a autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, e em cujo território a entrevista tiver lugar. Se solicitado pela referida autoridade, seus funcionários poderão auxiliar os funcionários e outras pessoas que os acompanhem, mediante autorização da Comissão, a conduzir a entrevista.

Artigo 23

Competências para realizar inspeções

1. Para desempenhar as suas funções ao abrigo do presente regulamento, a Comissão pode realizar todas as inspeções necessárias às empresas ou associações de empresas.

2. Os funcionários e outras pessoas que os acompanhem com autorização da Comissão para realizar uma inspeção estarão autorizados a:

a) acesso a quaisquer instalações, terrenos e meios de transporte das empresas e associações de empresas;

b) examinar livros e outros documentos relativos à atividade empresarial, independentemente do suporte em que se encontrem armazenados;

c) fazer ou obter cópias ou extratos, em qualquer formato, de tais livros ou documentos;

(d) exigir que a empresa ou associação de empresas forneça acesso e explicações sobre sua organização, operação, sistema de computador, algoritmos, gerenciamento de dados e práticas comerciais, e registre ou documente as explicações obtidas por quaisquer meios técnicos;

e) lacrar todas as dependências e livros ou documentos da empresa durante o período da vistoria e na medida necessária para tal;

f) solicitar a qualquer representante ou funcionário da empresa ou associação de empresas esclarecimentos sobre fatos ou documentos relacionados ao objeto e finalidade da vistoria, registrando suas respostas por qualquer meio técnico.

3. Para realizar inspeções, a Comissão pode solicitar a assistência de auditores ou peritos nomeados pela Comissão em conformidade com o artigo 26.º, n.º 2, e a assistência da autoridade nacional competente do Estado-Membro em cujo território a inspeção será realizada, responsável pela aplicação das regras referidas no artigo 1.º, n.º 6.

4. Durante as inspeções, a Comissão, os auditores ou peritos por ela nomeados e a autoridade nacional competente do Estado-Membro em cujo território a inspeção será realizada, responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, podem exigir que a empresa ou associação de empresas forneça acesso e explicações sobre a sua organização, funcionamento, sistema informático, algoritmos, gestão de dados e práticas comerciais. A Comissão e os auditores ou peritos por ela nomeados, bem como a autoridade nacional competente do Estado-Membro em cujo território a inspeção será efectuada e responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, podem colocar perguntas a qualquer representante ou membro do pessoal.

5. Os funcionários e outras pessoas que os acompanhem, com autorização da Comissão para realizar uma inspeção, exercerão os seus poderes mediante a apresentação de uma autorização escrita que indique o objeto e a finalidade da inspeção e as sanções previstas no artigo 30.º, no caso de os livros ou outros documentos exigidos relativamente à atividade empresarial serem apresentados de forma incompleta ou no caso de as respostas às questões colocadas em aplicação dos n.ºs 2 e 4 do presente artigo serem inexatas ou enganosas. A Comissão notificará atempadamente a autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, em cujo território a inspeção deverá ser efectuada.

6. As empresas ou associações de empresas são obrigadas a submeter-se a uma inspeção ordenada por decisão da Comissão. A decisão especificará o objeto e a finalidade da inspeção, fixará a data de seu início e indicará as multas e sanções pecuniárias compulsórias previstas nos artigos 30 e 31, respectivamente, bem como a possibilidade de revisão da decisão pelo Tribunal de Justiça.

7. Os funcionários da autoridade nacional competente do Estado-Membro em cujo território a inspeção será realizada e responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6, e qualquer pessoa autorizada ou nomeada por essa autoridade nacional devem, a pedido dessa autoridade ou da Comissão, prestar assistência ativa aos funcionários e outras pessoas que os acompanhem com a autorização da Comissão. Para tanto, gozarão das faculdades estabelecidas nos parágrafos 2 e 4 deste artigo.

8. Sempre que os funcionários e outras pessoas que os acompanhem com a autorização da Comissão verificarem que uma empresa ou associação de empresas se opõe a uma inspeção ordenada ao abrigo do presente artigo, o Estado-Membro em causa deve prestar-lhes a assistência necessária, solicitando, se for caso disso, a ação da polícia ou de uma força ou organismo de segurança equivalente, para lhes permitir efetuar a inspeção.

9. Sempre que, nos termos da legislação nacional, a assistência prevista no n.º 8 do presente artigo exija autorização judicial, a Comissão ou a autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, ou os funcionários autorizados por essas autoridades devem solicitá-la. Esta autorização também poderá ser solicitada como medida de precaução.

10. Ao solicitar a autorização prevista no parágrafo 9 deste artigo, a autoridade judiciária nacional verificará a autenticidade da decisão da Comissão e se as medidas coercitivas previstas não são arbitrarias ou desproporcionais ao objeto da inspeção. Na sua análise da proporcionalidade das medidas coercivas, a autoridade judicial nacional pode solicitar à Comissão, diretamente ou através da autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, explicações pormenorizadas sobre, em especial, os motivos pelos quais a Comissão suspeita que o presente regulamento foi violado, bem como a gravidade da alegada infração e a natureza do envolvimento da empresa em causa. Contudo, a autoridade judiciária nacional não pode impor a necessidade de uma inspeção ou exigir que as informações contidas no processo da Comissão lhe sejam submetidas. A legalidade da decisão da Comissão só estará sujeita à revisão do Tribunal de Justiça.

Artigo 24

Medidas de precaução

Em caso de urgência devido ao risco de danos graves e irreparáveis para os utilizadores profissionais ou utilizadores finais dos controladores de acesso, a Comissão pode adoptar um acto de execução que ordene medidas cautelares contra um controlador de acesso com base numa verificação da existência de primeira vista de uma infracção aos artigos 5.º, 6.º ou 7.º. Tal acto de execução só será adoptado no âmbito de um procedimento iniciado com vista à possível adopção de uma decisão nos termos do artigo 29.º(1). Só será aplicável por um período de tempo especificado e poderá ser renovado na medida do necessário e adequado. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

Artigo 25

Compromissos

1. Sempre que, durante o procedimento referido no artigo 18.º, o controlador de acesso se oferecer para assumir compromissos relativamente aos serviços essenciais de plataforma relevantes, a fim de garantir o cumprimento das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º, a Comissão pode adotar um ato de execução que torne esses compromissos vinculativos para esse controlador de acesso e declare que não existem mais motivos para ação. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

2. A Comissão pode, a pedido ou por sua própria iniciativa, reabrir o procedimento quando:

- a) tenha havido alteração da situação de facto relativamente a um elemento essencial da decisão;
- b) o porteiro em causa não cumprir as suas obrigações;
- c) a decisão foi baseada em informações incompletas, inexatas ou enganosas fornecidas pelas partes;
- d) os compromissos não sejam efetivados.

3. Se a Comissão considerar que os compromissos apresentados pelo controlador de acesso em causa não podem garantir o cumprimento efetivo das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º, deve explicar as razões pelas quais esses compromissos não são vinculativos na decisão relevante que encerra o procedimento.

Artigo 26

Controle de obrigações e medidas

1. A Comissão tomará as medidas necessárias para monitorizar a aplicação efectiva e o cumprimento das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º e das decisões tomadas nos termos dos artigos 8.º, 18.º, 24.º, 25.º e 29.º. Essas medidas incluirão, em especial, a imposição aos controladores de acesso da obrigação de conservar todos os documentos considerados relevantes para verificar a aplicação e o cumprimento dessas obrigações e decisões.

2. As ações previstas no n.º 1 podem incluir a nomeação de peritos e auditores externos independentes, bem como a nomeação de funcionários das autoridades nacionais competentes dos Estados-Membros, para assistir a Comissão na monitorização das obrigações e medidas e para lhe fornecer conhecimentos ou competências específicas.

Artigo 27

Informações de terceiros

1. Qualquer terceiro, incluindo utilizadores profissionais, concorrentes ou utilizadores finais de serviços essenciais de plataforma enumerados na decisão de designação nos termos do artigo 3.º, n.º 9, bem como os seus representantes, pode comunicar à autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, ou diretamente à Comissão, qualquer prática ou comportamento dos controladores de acesso abrangidos pelo âmbito de aplicação do presente regulamento.

2. A autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, e a Comissão terão plena discricção quanto às medidas adequadas e não serão obrigadas a dar seguimento às informações recebidas.

3. Sempre que a autoridade nacional competente do Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, determinar, com base nas informações recebidas nos termos do n.º 1 do presente artigo, que poderá existir um problema de incumprimento do presente regulamento, deve transmitir essas informações à Comissão.

Artigo 28

Função de verificação de conformidade

1. Os gatekeepers devem estabelecer uma função de verificação de conformidade que seja independente de suas funções operacionais e deve consistir em um ou mais responsáveis pela conformidade, incluindo a pessoa responsável pela função de verificação de conformidade.

2. O controlador de acesso deve garantir que a função de execução referida no parágrafo 1 tenha autoridade, dimensão e recursos suficientes, bem como acesso ao órgão de administração do controlador de acesso, para monitorizar o cumprimento do presente regulamento pelo controlador de acesso.

3. O órgão de administração do controlador deve garantir que os agentes de verificação nomeados nos termos do parágrafo 1 tenham as qualificações profissionais, os conhecimentos, a experiência e a capacidade necessárias para desempenhar as funções referidas no parágrafo 5.

O órgão dirigente do gatekeeper também deve garantir que a pessoa responsável pela função de verificação de conformidade seja um gerente sênior independente com responsabilidade específica pela função de verificação de conformidade.

4. A pessoa responsável pela função de execução deve reportar diretamente ao órgão dirigente do controlador e pode comunicar preocupações e advertências ao controlador sempre que houver risco de não conformidade com o presente regulamento, sem prejuízo das responsabilidades do órgão dirigente nas suas funções de supervisão e gestão.

O responsável pela função de verificação de conformidade não poderá ser substituído sem a aprovação prévia do órgão regulador do gatekeeper.

5. Os responsáveis pela conformidade nomeados pelo controlador nos termos do n.º 1 terão as seguintes funções:

(a) organizar, supervisionar e controlar as medidas e atividades dos controladores de acesso destinadas a garantir o cumprimento do presente regulamento;

b) informar e aconselhar a direção e os funcionários do porteiro sobre o cumprimento do presente Regulamento;

(c) sempre que adequado, monitorizar o cumprimento dos compromissos tornados vinculativos nos termos do artigo 25.º, sem prejuízo da capacidade da Comissão de nomear peritos externos independentes nos termos do artigo 26.º(2);

(d) cooperar com a Comissão para efeitos do presente regulamento.

6. Os controladores devem comunicar à Comissão o nome e os dados de contacto da pessoa responsável pela função de verificação da conformidade.

7. O órgão dirigente do gatekeeper deverá definir, supervisionar e ser responsável pela implementação dos acordos de governança do gatekeeper que garantam a independência da função de conformidade, incluindo a alocação de responsabilidades dentro da organização do gatekeeper e a prevenção de conflitos de interesse.

8. O órgão de administração aprovará e revisará periodicamente, pelo menos uma vez por ano, as estratégias e políticas destinadas a assumir, gerir e controlar o cumprimento do presente Regulamento.

9. O órgão de gestão deve dedicar tempo suficiente à gestão e monitorização do cumprimento do presente regulamento. Participará ativamente nas decisões relativas à gestão e à implementação do presente regulamento e assegurará que sejam atribuídos recursos adequados a estas tarefas.

Artigo 29

Violação

1. A Comissão adota um ato de execução que estabeleça as suas conclusões sobre o incumprimento (a seguir designado por «decisão de incumprimento») sempre que verificar que um controlador de acesso não cumpre uma ou mais das seguintes condições:

- a) qualquer das obrigações previstas nos artigos 5.º, 6.º ou 7.º;
- (b) as medidas especificadas pela Comissão numa decisão adoptada nos termos do artigo 8.º(2);
- (c) medidas corretivas impostas nos termos do artigo 18(1);
- (d) as medidas cautelares ordenadas nos termos do artigo 24.º, ou
- (e) compromissos que tenham sido tornados juridicamente vinculativos nos termos do artigo 25.º.

Esses atos de execução serão adotados pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

2. A Comissão deve esforçar-se por adoptar a sua decisão sobre a infracção no prazo de doze meses a contar do início do procedimento nos termos do artigo 20.º.

3. Antes de adotar a decisão de não conformidade, a Comissão comunicará as suas conclusões preliminares ao controlador em causa. Nessas conclusões preliminares, a Comissão deverá explicar as medidas que está considerando tomar ou considera que o controlador deve tomar para abordar eficazmente as conclusões preliminares.

4. A Comissão pode consultar terceiros quando pretender adotar uma decisão sobre o incumprimento.

5. Na decisão de não conformidade, a Comissão ordenará ao controlador que cesse a não conformidade dentro de um prazo adequado e forneça explicações sobre como pretende cumprir essa decisão.

6. O controlador deve fornecer à Comissão uma descrição das medidas que tomou para garantir o cumprimento da decisão de não conformidade.

7. Caso a Comissão decida não adotar uma decisão sobre o incumprimento, encerrará o procedimento por meio de uma decisão.

Artigo 30

Multas de penalidade

1. Na sua decisão sobre o incumprimento, a Comissão pode impor a um controlador multas não superiores a 10% do seu volume de negócios mundial total no exercício financeiro anterior, sempre que tenha constatado que o controlador está a falhar, intencionalmente ou por negligência:

- a) qualquer das obrigações previstas nos artigos 5.º, 6.º e 7.º;
- (b) as medidas especificadas pela Comissão numa decisão adoptada nos termos do artigo 8.º(2);
- (c) medidas corretivas impostas nos termos do artigo 18(1);
- (d) as medidas cautelares ordenadas nos termos do artigo 24.º, ou
- (e) compromissos que tenham sido tornados juridicamente vinculativos nos termos do artigo 25.º.

2. Em derrogação do parágrafo 1 deste artigo, na decisão de infração, a Comissão pode impor a um controlador de acesso multas de até 20% do seu volume de negócios mundial total no exercício financeiro anterior, caso tenha constatado em uma decisão de infração que um controlador de acesso cometeu a mesma infração de uma obrigação estabelecida no artigo 5, 6 ou 7 em relação ao mesmo serviço essencial de plataforma que já foi constatada em uma decisão de infração tomada durante os oito anos anteriores, ou uma infração semelhante.

3. A Comissão pode adoptar uma decisão que imponha às empresas, incluindo, se for caso disso, os controladores de acesso e as associações de empresas, multas não superiores a 1 % do seu volume de negócios mundial total no exercício financeiro anterior, sempre que, intencionalmente ou por negligência:

(a) não fornecer dentro do prazo as informações necessárias para verificar a sua designação como controladores de acesso, nos termos do artigo 3.º, ou fornecer informações incorretas, incompletas ou enganosas;

(b) não cumprir a obrigação de notificar a Comissão nos termos do artigo 3.º(3);

(c) não notificar as informações exigidas nos termos do artigo 14.º ou as informações que fornecerem nos termos desse artigo forem incorretas, incompletas ou enganosas;

(d) não forneçam a descrição exigida pelo artigo 15.º ou as informações que forneçam sejam incorretas, incompletas ou enganosas;

(e) não facultar acesso a bases de dados, algoritmos ou informações sobre testes em resposta a um pedido nos termos do artigo 21.º(3);

(f) não fornecer, no prazo especificado no artigo 21(3), as informações solicitadas ou fornecer informações ou explicações incorretas, incompletas ou enganosas solicitadas nos termos do artigo 21 ou fornecidas numa entrevista nos termos do artigo 22;

(g) não retificar, no prazo fixado pela Comissão, informações incorretas, incompletas ou enganosas fornecidas por um representante ou membro do pessoal, ou não fornecer ou recusar-se a fornecer informações completas sobre factos relacionados com o objeto e a finalidade de uma inspeção, nos termos do artigo 23.º;

(h) recusar-se a submeter-se a uma inspeção nos termos do artigo 23.º;

(i) não cumprir as obrigações impostas pela Comissão nos termos do artigo 26.º;

(j) não estabelecer a função de verificação da conformidade nos termos do artigo 28.º, ou

(k) não preencher as condições de acesso ao processo da Comissão, nos termos do artigo 34.º(4).

4. Ao fixar o montante da multa, a Comissão terá em conta a gravidade, a duração, a reiteração e, no caso de sanções impostas nos termos do n.º 3, o atraso causado ao procedimento.

5. Quando uma multa for imposta a uma associação de empresas tendo em conta o volume de negócios mundial dos seus membros e a associação não for solvente, esta será obrigada a pedir aos seus membros contribuições para cobrir o montante da multa.

Caso tais contribuições não tenham sido feitas à associação de empresas dentro de um prazo fixado pela Comissão, a Comissão pode exigir o pagamento da multa diretamente de qualquer uma das empresas cujos representantes tenham sido membros dos órgãos sociais relevantes dessa associação.

Após ter exigido o pagamento de acordo com o segundo parágrafo, a Comissão pode exigir o pagamento do saldo de qualquer um dos membros da associação de empresas, quando isso for necessário para garantir o pagamento integral da multa.

No entanto, a Comissão não exigirá o pagamento previsto no segundo ou terceiro parágrafos às empresas que demonstrem não ter aplicado a decisão da associação de empresas que violou o presente regulamento e que desconheciam a sua existência ou se tinham distanciado ativamente da mesma antes de a Comissão ter iniciado o procedimento nos termos do artigo 20.º.

A responsabilidade financeira de cada empresa pelo pagamento da multa não excederá 20% do seu faturamento mundial total no ano fiscal anterior.

Artigo 31

Multas coercitivas

1. A Comissão pode adotar uma decisão que imponha às empresas, incluindo, quando aplicável, os controladores de acesso e as associações de empresas, sanções pecuniárias periódicas diárias não superiores a 5 % do seu volume de negócios médio diário a nível mundial no exercício financeiro anterior, calculado a partir da data fixada por essa decisão, a fim de as obrigar a:

- (a) cumprir as medidas especificadas pela Comissão com base numa decisão tomada nos termos do artigo 8.º(2);
- b) cumprir a decisão tomada nos termos do artigo 18.º(1);
- (c) fornecer informações corretas e completas dentro do prazo exigido por um pedido de informações feito por meio de uma decisão adotada nos termos do artigo 21;
- (d) garantir o acesso a bases de dados, algoritmos e informações sobre testes em resposta a um pedido efetuado nos termos do artigo 21.º, n.º 3, e fornecer explicações sobre os mesmos, conforme solicitado por uma decisão tomada nos termos do artigo 21.º;
- (e) submeter-se a uma inspeção ordenada por decisão tomada nos termos do artigo 23.º;
- (f) cumprir uma decisão que ordene medidas cautelares tomadas nos termos do artigo 24.º;
- (g) cumprir compromissos que tenham sido tornados juridicamente vinculativos por uma decisão adotada nos termos do artigo 25.º(1);
- (h) cumprir uma decisão tomada nos termos do artigo 29(1).

2. Sempre que as empresas, ou associações de empresas, tenham cumprido a obrigação que a sanção pecuniária compulsória pretendia impor, a Comissão pode adotar um ato de execução que fixe o montante final da sanção pecuniária compulsória num valor inferior ao que resultaria da decisão inicial. Esse ato de execução será adotado pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

Artigo 32

Prazos de prescrição para a imposição de sanções

1. Os poderes conferidos à Comissão pelos artigos 30.º e 31.º prescrevem em cinco anos.
2. O prazo começa a correr a partir do dia em que a infração é cometida. Contudo, no caso de infrações continuadas ou repetidas, o prazo começará a correr no dia em que a infração cessar.
3. Qualquer medida tomada pela Comissão para efeitos de investigação de mercado ou de procedimento de infração interromperá o prazo de prescrição para a aplicação de multas ou sanções pecuniárias compulsórias. O prazo de prescrição interrompe-se a partir da data em que a ação for notificada a pelo menos uma empresa ou associação de empresas que tenha participado na infração. As ações que interrompem o curso do prazo incluem, em especial, as seguintes:

- (a) pedidos de informação à Comissão;
- (b) autorizações escritas para realizar inspeções emitidas pela Comissão aos seus funcionários;
- (c) o início de um procedimento pela Comissão nos termos do artigo 20.º.

4. Após cada interrupção, o prazo começará a ser contado desde o início. Contudo, o prazo de prescrição expirará, o mais tardar, no dia em que tiver decorrido um período igual ao dobro do prazo de prescrição sem que a Comissão tenha imposto uma multa ou uma sanção pecuniária compulsória. Este prazo será prorrogado pelo período de suspensão do prazo de prescrição nos termos do parágrafo 5.

5. O prazo de prescrição para a aplicação de multas ou sanções pecuniárias compulsórias fica suspenso enquanto a decisão da Comissão for objecto de recurso perante o Tribunal de Justiça.

Artigo 33

Prazos de prescrição para a execução de sanções

1. Os poderes da Comissão para executar decisões tomadas nos termos dos artigos 30.º e 31.º estão sujeitos a um prazo de prescrição de cinco anos.
2. O prazo começa a correr a partir do dia em que a decisão se torna definitiva.
3. O prazo de prescrição para execução das sanções interrompe-se:
 - (a) por notificação de uma decisão que altere o montante inicial da multa ou da sanção pecuniária compulsória ou que rejeite um pedido de alteração, ou
 - (b) por qualquer ato da Comissão ou de um Estado-Membro agindo a pedido da Comissão, que vise recuperar, por meio da execução, a multa ou a sanção pecuniária compulsória.
4. Após cada interrupção, o prazo começará a ser contado desde o início.
5. O prazo de prescrição da execução das sanções suspende-se enquanto:
 - a) perdurar o prazo concedido para a realização do pagamento, ou
 - (b) a suspensão do processo de execução por força de uma decisão do Tribunal de Justiça ou de uma decisão de um tribunal nacional perdurar.

Artigo 34

Direito de ser ouvido e acesso ao processo

1. Antes de adotar uma decisão nos termos do artigo 8.º, do artigo 9.º(1), do artigo 10.º(1), dos artigos 17.º, 18.º, 24.º, 25.º, 29.º, 30.º e do artigo 31.º(2), a Comissão deve dar ao controlador de acesso ou à empresa ou associação de empresas em causa a oportunidade de ser ouvido relativamente ao seguinte:
 - (a) as conclusões preliminares da Comissão, incluindo quaisquer questões às quais a Comissão tenha levantado objecções, e
 - (b) as medidas que a Comissão pretende tomar à luz das conclusões preliminares nos termos da alínea a) do presente número.
2. Os controladores, empresas e associações de empresas em causa podem apresentar à Comissão as suas observações sobre as conclusões preliminares da Comissão num prazo a fixar pela Comissão nas suas conclusões preliminares, que não pode ser inferior a catorze dias.

3. A Comissão baseará as suas decisões exclusivamente em conclusões preliminares, incluindo quaisquer questões às quais tenha levantado objeções e sobre as quais os controladores, as empresas e as associações de empresas em causa tenham podido comentar.

4. Em todos os procedimentos, os direitos de defesa do porteiro, da empresa ou associação de empresas em causa serão integralmente respeitados. O controlador, empresa ou associação de empresas em causa terá o direito de aceder ao processo da Comissão em condições de divulgação, sem prejuízo do interesse legítimo das empresas em proteger os seus segredos comerciais. Em caso de desacordo entre as partes, a Comissão poderá adotar decisões que estabeleçam tais condições de divulgação. O direito de acesso ao processo da Comissão não se estende às informações confidenciais ou aos documentos internos da Comissão ou das autoridades competentes dos Estados-Membros. Em particular, o direito de acesso não se estende às trocas de correspondência entre a Comissão e as autoridades competentes dos Estados-Membros. Nada neste parágrafo impedirá a Comissão de divulgar e utilizar informações necessárias para provar uma infração.

Artigo 35

Relatórios anuais

1. A Comissão apresentará ao Parlamento Europeu e ao Conselho um relatório anual sobre a aplicação do presente regulamento e os progressos realizados na consecução dos seus objetivos.

2. O relatório referido no n.º 1 deve incluir:

- (a) um resumo das atividades da Comissão, incluindo quaisquer medidas ou decisões tomadas e investigações de mercado em curso relacionadas com o presente regulamento;
- (b) as conclusões retiradas da monitorização do cumprimento das obrigações que lhes incumbem por força do presente regulamento pelos controladores de acesso;
- (c) uma avaliação da descrição auditada referida no artigo 15.º;
- (d) uma visão geral da cooperação entre a Comissão e as autoridades nacionais no que diz respeito ao presente regulamento;
- (e) uma visão geral das atividades e tarefas realizadas pelo Grupo de Alto Nível de Reguladores Digitais, indicando como as suas recomendações devem ser implementadas no que diz respeito à implementação do presente regulamento.

3. A Comissão publicará o relatório no seu sítio Web.

Artigo 36

Sigilo profissional

1. As informações recolhidas nos termos do presente regulamento serão utilizadas para os fins do presente regulamento.

2. As informações recolhidas nos termos do artigo 14.º serão utilizadas para efeitos do presente regulamento, o Regulamento (CE) n.º ^{qualquer}139/2004 e regulamentos nacionais sobre concentrações.

3. As informações recolhidas nos termos do artigo 15.º serão utilizadas para efeitos do presente regulamento e do Regulamento (UE) 2016/679.

4. Sem prejuízo da troca e utilização de informações fornecidas para efeitos do presente regulamento nos termos dos artigos 38.º, 39.º, 41.º e 43.º, a Comissão, as autoridades competentes dos Estados-Membros, os seus funcionários, agentes e outras pessoas que trabalhem sob a supervisão dessas autoridades, e qualquer pessoa singular ou coletiva, incluindo auditores e peritos nomeados nos termos do artigo 26.º(2), são obrigados a não divulgar informações que tenham recolhido ou trocado em aplicação do presente regulamento e que, pela sua natureza, estejam abrangidas pelo sigilo profissional.

Artigo 37

Cooperação com autoridades nacionais

1. A Comissão e os Estados-Membros devem trabalhar em estreita cooperação e coordenar as suas ações de execução para garantir uma implementação coerente, eficaz e complementar dos instrumentos jurídicos disponíveis aplicáveis aos controladores de acesso, na aceção do presente regulamento.
2. Sempre que adequado, a Comissão pode consultar as autoridades nacionais sobre qualquer questão relacionada com a aplicação do presente regulamento.

Artigo 38

Cooperação e coordenação com as autoridades nacionais competentes responsáveis pela aplicação das regras em questões de concorrência

1. A Comissão e as autoridades nacionais competentes dos Estados-Membros responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6, cooperam e informam-se mutuamente sobre as respetivas medidas de aplicação através da Rede Europeia da Concorrência (REC). Eles terão poderes para comunicar entre si quaisquer informações sobre questões de fato e de direito, incluindo informações confidenciais. Quando a autoridade competente não for membro da ECN, a Comissão tomará as disposições necessárias para a cooperação e a troca de informações sobre questões relacionadas com a implementação do presente regulamento e das regras referidas no artigo 1.º, n.º 6. A Comissão pode estabelecer tais disposições num ato de execução, conforme referido no artigo 46.º, n.º 1, alínea l).
2. Sempre que a autoridade nacional competente de um Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, pretenda iniciar uma investigação sobre os controladores de acesso com base na legislação nacional referida no artigo 1.º, n.º 6, deve informar a Comissão por escrito da sua primeira medida formal de investigação, antes ou imediatamente após o início dessa medida. Estas informações podem também ser disponibilizadas às autoridades nacionais competentes dos outros Estados-Membros responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6.
3. Sempre que a autoridade nacional competente de um Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, pretenda impor obrigações aos controladores de acesso com base na legislação nacional referida no artigo 1.º, n.º 6, deverá, o mais tardar 30 dias antes da sua adoção, comunicar à Comissão o projeto de medidas, indicando as razões que as justificam. No caso de medidas de precaução, a autoridade nacional competente de um Estado-Membro responsável pela execução das regras referidas no artigo 1.º, n.º 6, deve comunicar à Comissão o projeto das medidas previstas o mais rapidamente possível e, o mais tardar, imediatamente após a adoção dessas medidas. Estas informações podem também ser disponibilizadas às autoridades nacionais competentes dos outros Estados-Membros responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6.
4. Os mecanismos de informação previstos nos n.os 2 e 3 não se aplicam às decisões previstas nas regras nacionais em matéria de concentrações.
5. As informações trocadas nos termos dos n.ºs 1 a 3 do presente artigo só serão trocadas e utilizadas para efeitos de coordenação da aplicação do presente regulamento e das regras referidas no artigo 1.º, n.º 6.
6. A Comissão pode solicitar às autoridades nacionais competentes dos Estados-Membros responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6, que apoiem qualquer uma das suas investigações de mercado nos termos do presente regulamento.
7. Sempre que, ao abrigo da legislação nacional, a autoridade nacional competente de um Estado-Membro responsável pela aplicação das regras referidas no artigo 1.º, n.º 6, tiver o poder e os poderes de investigação para o fazer, pode, por sua própria iniciativa, investigar casos de possível incumprimento dos artigos 5.º, 6.º e 7.º do presente regulamento no seu território. Antes de tomar a primeira medida formal de investigação, a referida autoridade deverá informar a Comissão por escrito.

O início de um procedimento pela Comissão nos termos do artigo 20.º privará as autoridades nacionais competentes dos Estados-Membros responsáveis pela aplicação das regras referidas no artigo 1.º, n.º 6, do poder de realizar tal investigação, ou encerrará tal investigação se já estiver em curso. Essas autoridades informarão a Comissão sobre as conclusões dessa investigação, a fim de apoiar a Comissão no seu papel de única autoridade responsável pela aplicação do presente regulamento.

Artigo 39

Cooperação com tribunais nacionais

1. Nos processos de aplicação do presente regulamento, os tribunais nacionais podem solicitar à Comissão que lhes forneça informações na sua posse ou um parecer sobre questões relacionadas com a aplicação do presente regulamento.
2. Os Estados-Membros devem enviar à Comissão uma cópia de todas as decisões proferidas por um tribunal nacional sobre a aplicação do presente regulamento. Esta cópia será encaminhada sem demora após a notificação às partes do texto integral da sentença.
3. Sempre que a aplicação coerente do presente regulamento o exigir, a Comissão pode, oficiosamente, dirigir observações escritas aos tribunais nacionais. Mediante autorização do órgão judiciário competente, poderão também ser apresentadas observações verbais.
4. Com o único propósito de preparar as suas observações, a Comissão pode solicitar ao tribunal nacional em causa que transmita ou assegure a transmissão de toda a documentação necessária à apreciação do caso.
5. Os tribunais nacionais não podem adotar decisões contrárias a uma decisão tomada pela Comissão nos termos do presente regulamento. Devem também evitar adotar decisões que possam entrar em conflito com uma decisão prevista pela Comissão num procedimento que esta já tenha iniciado ao abrigo do presente regulamento. Para esse efeito, cabe aos tribunais nacionais determinar se os seus processos devem ser suspensos. Isto não prejudica a possibilidade de os tribunais nacionais apresentarem um pedido de decisão prejudicial nos termos do artigo 267.º do TFUE.

Artigo 40

O Grupo de Alto Nível

1. A Comissão criará um Grupo de Alto Nível sobre a Regulamentação dos Mercados Digitais (a seguir designado por «Grupo de Alto Nível»).
2. O Grupo de Alto Nível será composto pelas seguintes redes e organismos europeus:
 - a) Organismo de Reguladores Europeus das Comunicações Eletrónicas;
 - b) Autoridade Europeia para a Proteção de Dados e Comité Europeu para a Proteção de Dados;
 - c) Rede Europeia da Concorrência;
 - d) Rede de cooperação em matéria de protecção do consumidor, e
 - e) Grupo de Entidades Reguladoras Europeias de Serviços de Comunicação Social Audiovisual.
3. As redes e os organismos europeus referidos no n.º 2 terão cada um um número igual de representantes no Grupo de Alto Nível. O Grupo de Alto Nível terá no máximo trinta membros.
4. A Comissão fornecerá serviços de secretaria ao Painel de Alto Nível para facilitar seu trabalho. O Grupo de Alto Nível será presidido pela Comissão, que participará de suas reuniões. O Grupo de Alto Nível reunir-se-á a pedido da Comissão pelo menos uma vez por ano civil. A Comissão também convocará uma reunião do grupo quando solicitada pela maioria dos seus membros para tratar de uma questão específica.

5. O Grupo de Alto Nível pode fornecer à Comissão aconselhamento e conhecimentos especializados em áreas de competência dos seus membros, em particular:

- (a) aconselhamento e recomendações baseadas na sua experiência relevante para qualquer questão de natureza geral relacionada com a aplicação ou execução do presente regulamento, ou
- b) aconselhamento e experiência que promovam uma abordagem regulatória coerente entre diferentes instrumentos regulatórios.

6. O Grupo de Alto Nível pode, em particular, identificar e examinar as interações atuais e potenciais entre o presente regulamento e as regras setoriais aplicadas pelas autoridades nacionais que compõem as redes e organismos europeus referidos no n.º 2, e apresentar um relatório anual à Comissão que reflita esse exame e registre quaisquer dificuldades interregulatórias. Este relatório pode ser acompanhado de recomendações destinadas a alcançar sinergias e abordagens interdisciplinares coerentes entre a aplicação deste Regulamento e outras regras setoriais. O relatório será submetido ao Parlamento Europeu e ao Conselho.

7. No contexto de investigações de mercado sobre novos serviços e novas práticas, o Grupo de Alto Nível pode fornecer conhecimentos especializados à Comissão sobre a necessidade de adicionar regras ao presente Regulamento ou de alterar ou remover regras do presente Regulamento, a fim de garantir que os mercados digitais em toda a União sejam contestáveis e justos.

Artigo 41

Solicitação de pesquisa de mercado

1. Três ou mais Estados-Membros podem solicitar à Comissão que abra uma investigação de mercado nos termos do artigo 17.º, com base na existência de motivos razoáveis para crer que uma empresa deve ser designada como controladora de acesso.

2. Um ou mais Estados-Membros podem solicitar à Comissão que inicie uma investigação de mercado nos termos do artigo 18.º, com base no facto de existirem motivos razoáveis para crer que um controlador de acesso não cumpriu sistematicamente uma ou mais das obrigações estabelecidas nos artigos 5.º, 6.º e 7.º e manteve, reforçou ou alargou a sua posição de controlador de acesso em relação aos requisitos estabelecidos no artigo 3.º(1).

3. Três ou mais Estados-Membros podem solicitar à Comissão que realize uma investigação de mercado nos termos do artigo 19.º, com base na existência de motivos razoáveis para crer que:

- a) um ou mais serviços do sector digital devem ser acrescentados à lista de serviços essenciais de plataforma estabelecida no artigo 2.º, ponto 2, ou
- (b) uma ou mais práticas que possam limitar a disputabilidade dos serviços essenciais da plataforma ou ser desleais não sejam abordadas de forma eficaz no presente regulamento.

4. Os Estados-Membros devem fornecer provas para apoiar os seus pedidos, em conformidade com os n.ºs 1, 2 e 3. No caso de pedidos nos termos do n.º 3, essas provas podem incluir informações sobre ofertas de produtos, serviços, programas ou benefícios que levantam questões de contestabilidade ou justiça, sejam aplicados no contexto de serviços de plataforma principais existentes ou em outro lugar.

5. No prazo de quatro meses a contar da recepção de um pedido nos termos do presente artigo, a Comissão examinará se existem motivos razoáveis para iniciar uma investigação de mercado nos termos dos n.ºs 1, 2 ou 3. A Comissão publicará os resultados do seu exame.

Artigo 42

Ações de representação

A Diretiva (UE) 2020/1828 aplica-se às ações representativas intentadas contra atos de controladores de acesso que violem as disposições do presente regulamento e prejudiquem ou sejam suscetíveis de prejudicar os interesses coletivos dos consumidores.

Artigo 43

Denúncia de infrações e proteção de denunciantes

A Diretiva (UE) 2019/1937 aplica-se à comunicação de todas as violações do presente regulamento e à proteção das pessoas que comunicam tais violações.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Artigo 44

Publicação de decisões

1. A Comissão publicará as decisões que adotar nos termos dos artigos 3.º e 4.º, do artigo 8.º(2), dos artigos 9.º, 10.º, 16.º a 20.º e 24.º, do artigo 25.º(1) e dos artigos 29.º, 30.º e 31.º. Essa publicação indicará os nomes das partes e o conteúdo principal da decisão, incluindo quaisquer sanções impostas.

2. A publicação deve levar em consideração o interesse legítimo dos guardiões ou de terceiros em proteger suas informações confidenciais.

Artigo 45

Controle do Tribunal de Justiça

Nos termos do artigo 261.º do TFUE, o Tribunal de Justiça tem jurisdição ilimitada para rever decisões pelas quais a Comissão impôs multas ou sanções pecuniárias compulsórias. Poderá anular, reduzir ou aumentar a multa ou coima aplicada.

Artigo 46

Regras de desenvolvimento

1. A Comissão pode adotar atos de execução que estabeleçam disposições pormenorizadas para a implementação do seguinte:

- (a) a forma, o conteúdo e outros detalhes das notificações e informações apresentadas nos termos do artigo 3.º;
- (b) a forma, o conteúdo e outros detalhes das medidas técnicas que os controladores de acesso devem implementar para garantir o cumprimento dos artigos 5.º, 6.º ou 7.º;
- (c) aspectos operacionais e técnicos com vista à implementação da interoperabilidade dos serviços de comunicações interpessoais independentes do número, em conformidade com o artigo 7.º;
- (d) a forma, o conteúdo e outros detalhes do pedido fundamentado, nos termos do artigo 8.º, n.º 3;
- (e) a forma, o conteúdo e outros detalhes dos pedidos fundamentados nos termos dos artigos 9.º e 10.º;
- (f) a forma, o conteúdo e outros detalhes dos relatórios regulamentares apresentados nos termos do artigo 11.º;
- (g) a metodologia e o procedimento para a descrição auditada das técnicas utilizadas para a definição de perfis dos consumidores referida no artigo 15.º, n.º 1. Ao elaborar um projeto de ato de execução para estes fins, a Comissão deve consultar a Autoridade Europeia para a Proteção de Dados e pode consultar o Comité Europeu para a Proteção de Dados, a sociedade civil e outros peritos relevantes;
- (h) a forma, o conteúdo e outros detalhes das notificações e informações apresentadas nos termos dos artigos 14.º e 15.º;

- (i) as disposições práticas relativas aos procedimentos relativos às investigações de mercado, nos termos dos artigos 17.º, 18.º e 19.º, e aos procedimentos previstos nos artigos 24.º, 25.º e 29.º;
- (j) os aspectos práticos do exercício do direito de ser ouvido previsto no artigo 34.º;
- (k) os aspectos práticos das condições de divulgação previstas no artigo 34.º;
- (l) os aspectos práticos da cooperação e coordenação entre a Comissão e as autoridades nacionais referidas nos artigos 37.º e 38.º, e
- m) os aspectos práticos do cálculo e da prorrogação de prazos.

2. Os atos de execução referidos nas alíneas a) a k) e m) do n.º 1 do presente artigo são adotados pelo procedimento consultivo a que se refere o artigo 50.º, n.º 2.

O ato de execução referido na alínea l) do n.º 1 do presente artigo é adotado pelo procedimento de exame a que se refere o artigo 50.º, n.º 3.

3. Antes de adotar qualquer ato de execução nos termos do parágrafo 1, a Comissão publicará um projeto do ato e convidará todas as partes interessadas a apresentarem seus comentários dentro de um período não inferior a um mês.

Artigo 47

Diretrizes

A Comissão pode adotar diretrizes sobre qualquer aspecto do presente regulamento, a fim de facilitar sua aplicação e execução efetivas.

Artigo 48

Padronização

Sempre que adequado e necessário, a Comissão pode instruir as organizações europeias de normalização para facilitar o cumprimento das obrigações estabelecidas no presente regulamento através do desenvolvimento de normas adequadas.

Artigo 49

Exercício de delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.
2. O poder de adotar atos delegados referido no artigo 3.º, n.os 6 e 7, e no artigo 12.º, n.os 1, 3 e 4, será conferido à Comissão por um período de cinco anos a partir de 1 de novembro de 2022. A Comissão elaborará um relatório relativo à delegação de poderes o mais tardar nove meses antes do final do período de cinco anos. A delegação de poderes será tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada período.
3. A delegação de poderes referida no artigo 3.º, n.os 6 e 7, e no artigo 12.º, n.os 1, 3 e 4, pode ser revogada a qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão entrará em vigor no dia seguinte ao da sua publicação no Diário Oficial da União. Jornal Oficial da União Europeia ou em uma data posterior indicada nele. Não afetará a validade dos atos delegados já em vigor.
4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro, em conformidade com os princípios estabelecidos no Acordo Interinstitucional de 13 de abril de 2016 sobre legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Um ato delegado adotado nos termos do artigo 3.º, n.os 6 e 7, e do artigo 12.º, n.os 1, 3 e 4, só entrará em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O prazo será prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 50

Procedimento de comissão

1. A Comissão será assistida por um comité («Comité Consultivo sobre Mercados Digitais»). Este comité será um comité na acepção do Regulamento (UE) n.º ^{qualquer}182/2011.

2. Sempre que se faça referência ao presente número, aplica-se o artigo 4.º do Regulamento (UE).

n.º qualquer 182/2011.

Quando o parecer do comité tiver de ser obtido por procedimento escrito, o procedimento será encerrado sem resultados se, dentro do prazo para a emissão do parecer, o presidente do comité assim o decidir ou se a maioria simples dos membros do comité assim o solicitar.

3. Sempre que se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE).

n.º qualquer 182/2011.

4. A Comissão comunicará o parecer do comité ao destinatário de uma decisão individual, juntamente com essa decisão. Tornará pública a opinião juntamente com a decisão individual, tendo em conta o interesse legítimo de proteger o sigilo profissional.

Artigo 51

Emenda à Diretiva (UE) 2019/1937

Na Parte I, Secção J, do Anexo da Diretiva (UE) 2019/1937, é aditado o seguinte parágrafo:

«iv) Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo aos mercados e direito da concorrência leal no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais) (JO L 265 de 21.9.2022, p. 1).».

Artigo 52

Emenda à Diretiva (UE) 2020/1828

O seguinte ponto é aditado ao Anexo I da Diretiva (UE) 2020/1828:

«67) Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo aos mercados e direito da concorrência leal no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais) (JO L 265 de 21.9.2022, p. 1).».

Artigo 53

Revisão

1. Até 3 de maio de 2026 e, posteriormente, de três em três anos, a Comissão deve avaliar o presente regulamento e apresentar um relatório ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu.

2. As avaliações devem avaliar se os objetivos do presente regulamento, nomeadamente garantir mercados justos e contestáveis, foram alcançados e o impacto do presente regulamento nos utilizadores empresariais, em especial nas PME, e nos utilizadores finais. Além disso, a Comissão avaliará se o escopo do artigo 7 pode ser estendido aos serviços de redes sociais online.

3. As avaliações devem estabelecer se é necessário alterar as regras, em especial no que se refere à lista de serviços essenciais de plataforma estabelecida no ponto (2) do artigo 2.º ou às obrigações estabelecidas nos artigos 5.º, 6.º e 7.º e à sua implementação, a fim de garantir que os mercados digitais em toda a União sejam contestáveis e justos. Após as avaliações, a Comissão tomará medidas adequadas, que podem incluir propostas legislativas.

4. As autoridades competentes dos Estados-Membros devem fornecer à Comissão todas as informações pertinentes de que esta disponha e que esta possa necessitar para elaborar o relatório referido no n.º 1.

Artigo 54

Entrada em vigor e aplicação

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

Ela entrará em vigor em 2 de maio de 2023.

Contudo, o artigo 3.º, n.ºs 6 e 7, e os artigos 40.º, 46.º, 47.º, 48.º, 49.º e 50.º serão aplicáveis a partir de 1 de novembro de 2022, e os artigos 42.º e 43.º serão aplicáveis a partir de 25 de junho de 2023.

Contudo, se a data de 25 de junho de 2023 for anterior à data de aplicação referida no segundo parágrafo deste artigo, a aplicação do artigo 42.º e do artigo 43.º será adiada até à data de aplicação referida no segundo parágrafo deste artigo.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Estrasburgo, 14 de setembro de 2022.

Pelo Parlamento Europeu

O Presidente

R. METSOLA

Pelo Conselho

O Presidente

Senhor BEK

EXPOSIÇÃO

A. “Considerações gerais”

1. O presente anexo visa estabelecer uma metodologia para determinar e calcular os «utilizadores finais ativos» e os «utilizadores empresariais ativos» de cada serviço de plataforma principal, conforme enumerados no ponto (2) do artigo 2.º. Fornece um ponto de referência para uma empresa avaliar se os seus serviços de plataforma principais cumprem os limiares quantitativos estabelecidos no ponto (b) do artigo 3.º(2). Se assim for, presume-se que cumprem o requisito do artigo 3.º, n.º 1, alínea b). Este parâmetro de referência será, portanto, também relevante para qualquer avaliação mais ampla nos termos do Artigo 3(8). É da responsabilidade da empresa chegar à melhor aproximação possível, em conformidade com os princípios comuns e a metodologia específica definidos neste Anexo. Nada no presente anexo impede a Comissão de, dentro dos prazos estabelecidos nas disposições relevantes do presente regulamento, exigir que a empresa que fornece serviços essenciais de plataforma forneça as informações necessárias para identificar e calcular os «utilizadores finais ativos» e os «utilizadores empresariais ativos». Nada neste Anexo será considerado uma base legal para rastrear usuários. A metodologia estabelecida neste Anexo também não prejudica as obrigações estabelecidas no presente Regulamento, em particular no Artigo 3(3) e (8) e no Artigo 13(3). Em particular, o cumprimento necessário do Artigo 13(3) também implica a determinação e o cálculo de «utilizadores finais ativos» e de «utilizadores empresariais ativos» com base numa medição precisa ou na melhor aproximação disponível, em consonância com as capacidades reais de determinação e cálculo disponíveis para a empresa que fornece serviços essenciais de plataforma no momento em questão. Essas medições ou a melhor aproximação disponível devem ser consistentes e incluir os dados relatados nos termos do Artigo 15.
2. O artigo 2.º, n.ºs 20 e 21, contém as definições de “utilizador final” e “utilizador profissional”, que são comuns a todos os serviços básicos da plataforma.
3. Para efeitos de determinação e cálculo do número de “utilizadores finais ativos” e “utilizadores empresariais ativos”, este Anexo refere-se ao conceito de “utilizadores únicos”. O termo “usuários únicos” inclui “usuários finais ativos” e “usuários empresariais ativos” do serviço de plataforma principal relevante, contados apenas uma vez durante um determinado período de tempo (um mês para “usuários finais ativos” e um ano para “usuários empresariais ativos”), independentemente do número de vezes que interagiram com esse serviço de plataforma principal durante esse período. Isto não prejudica o fato de que a mesma pessoa física ou jurídica pode ser simultaneamente um usuário final ativo e um usuário profissional ativo de diferentes serviços básicos da plataforma.

B. “Usuários finais ativos”

1. O número de “usuários únicos” em relação aos “usuários finais ativos” será determinado com base na contagem mais precisa relatada pela empresa que fornece serviços básicos de plataforma, especificamente:
 - a. A coleta de dados sobre o uso dos principais serviços da plataforma em ambientes onde o registro ou login é necessário é considerada como apresentando, em princípio, o menor risco de duplicação, por exemplo, em relação ao comportamento do usuário em dispositivos ou plataformas. Por esse motivo, a Empresa apresentará dados agregados e anônimos sobre o número de usuários finais únicos de cada serviço principal da plataforma, extraídos de ambientes onde o registro ou login é necessário, se tais dados existirem.
 - b. Para serviços de plataforma principais que também são acessados por usuários finais fora dos ambientes de login/registo, a Empresa apresentará adicionalmente dados agregados anônimos sobre o número de usuários finais exclusivos do serviço de plataforma principal relevante, com base em uma contagem alternativa que também captura usuários finais fora dos ambientes de login/registo, por exemplo, com base em endereços IP, IDs de sessão na forma de cookies ou outros identificadores, como etiquetas de identificação por radiofrequência, desde que tais endereços ou identificadores sejam objetivamente necessários para o fornecimento de serviços básicos de plataforma.
2. O número de “usuários finais ativos mensais” é definido com base no número médio de usuários finais ativos mensais durante a maior parte do ano fiscal. O termo “a maior parte do ano” tem como objetivo permitir que um provedor de serviços de plataforma principais desconte valores discrepantes em um determinado ano. O

Números atípicos referem-se, como o próprio nome sugere, a números que estão significativamente fora dos números normais e esperados. Um aumento ou queda drástica e inesperada no engajamento do usuário durante um único mês do ano fiscal é um exemplo do que pode constituir um valor atípico. Números relacionados a eventos que ocorrem todos os anos, como promoções anuais de vendas, não são exceções.

C. "Usuários profissionais ativos"

O número de "usuários únicos" em relação aos "usuários empresariais ativos" deve ser determinado, quando aplicável, no nível da conta, onde cada conta empresarial distinta associada ao uso de um serviço de plataforma principal fornecido pela empresa é considerada um usuário empresarial exclusivo do respectivo serviço de plataforma principal. Se o termo "conta empresarial" não for aplicável a um serviço de plataforma principal específico, o número de usuários empresariais exclusivos será determinado pelo provedor de serviço de plataforma principal em questão, com referência ao negócio relevante.

D. «Apresentação de informação»

1. É da responsabilidade da empresa que, nos termos do artigo 3.º, n.º 3, apresenta à Comissão informações sobre o número de utilizadores finais ativos e de utilizadores empresariais ativos por serviço básico de plataforma garantir a integralidade e a exatidão dessas informações. Nesse sentido:

para. Será de responsabilidade da Empresa apresentar dados para o respectivo Serviço de Plataforma Principal que evitem a sub ou superestimação do número de usuários finais ativos e usuários comerciais ativos (por exemplo, se os usuários acessam os Serviços de Plataforma Principal por meio de diferentes plataformas ou dispositivos).

b. Será de responsabilidade da empresa fornecer explicações precisas e concisas sobre a metodologia utilizada para obtenção das informações e sobre qualquer risco de subestimação ou superestimação do número de usuários finais ativos e usuários profissionais ativos do respectivo serviço básico da plataforma, bem como sobre as soluções adotadas para lidar com tal risco.

c. A empresa deve fornecer dados baseados em um cálculo alternativo quando a Comissão tiver dúvidas sobre a exatidão dos dados fornecidos pela empresa que fornece serviços essenciais de plataforma.

2. Para efeitos de cálculo do número de "utilizadores finais ativos" e "utilizadores profissionais ativos":

para. O fornecedor de serviços de plataforma essenciais não deve considerar que os serviços de plataforma essenciais pertencentes à mesma categoria de serviços de plataforma essenciais, nos termos do ponto 2 do artigo 2.º, sejam diferentes com base no facto de serem fornecidos utilizando nomes de domínio diferentes, sejam eles domínios territoriais de nível superior (ccTLDs) ou domínios genéricos de nível superior (gTLDs), ou qualquer atributo geográfico.

b. O fornecedor de serviços essenciais de plataforma deve considerar como serviços essenciais de plataforma diferentes aqueles que são utilizados para finalidades diferentes pelos seus utilizadores finais, utilizadores empresariais ou ambos, mesmo que sejam os mesmos utilizadores finais ou utilizadores empresariais e mesmo que pertençam à mesma categoria de serviços essenciais de plataforma, nos termos do artigo 2.º, ponto 2.

c. A empresa prestadora de serviços básicos de plataforma considerará como serviços básicos de plataforma diferenciados aqueles serviços que a empresa em questão oferece de forma integrada, mas que:

(i) não pertencem à mesma categoria de serviços básicos de plataforma, em conformidade com o artigo 2.º, ponto 2, ou

(ii) são utilizados para finalidades diferentes pelos seus utilizadores finais, utilizadores empresariais ou ambos, mesmo que sejam os mesmos utilizadores finais e utilizadores empresariais e mesmo que pertençam à mesma categoria de serviços básicos de plataforma, nos termos do artigo 2.º, ponto 2.

E. "Definições específicas"

A tabela abaixo define definições específicas de "usuários finais ativos" e "usuários comerciais ativos" para cada serviço de plataforma principal.

Serviços básicos de plataforma	Usuários finais ativos	Usuários profissionais ativos
Serviços de corretagem online	Número de usuários finais únicos que interagiram com o serviço de intermediação on-line pelo menos uma vez durante o mês, por exemplo, efetuando login ativamente, fazendo uma consulta, clicando, rolando a página para baixo ou realizando transações por meio do serviço de intermediação on-line pelo menos uma vez durante o mês.	Número de usuários empresariais exclusivos que tiveram pelo menos um item listado no serviço de corretagem on-line durante o ano inteiro ou concluíram uma transação habilitada pelo serviço de corretagem on-line durante o ano.
Motores de busca on-line	Número de usuários finais únicos que interagiram com o mecanismo de busca on-line pelo menos uma vez durante o mês, por exemplo, fazendo uma consulta.	Número de usuários empresariais exclusivos com sites profissionais (ou seja, sites usados em caráter comercial ou profissional) adicionados ou já listados no índice do mecanismo de busca on-line durante o ano.
Serviços de redes sociais online	Número de usuários finais únicos que interagiram com o serviço de rede social on-line pelo menos uma vez durante o mês, por exemplo, efetuando login ativamente, abrindo uma página, rolando uma janela, clicando, curtindo, consultando, postando ou comentando.	Número de usuários empresariais únicos que anunciaram um produto ou serviço ou têm uma conta empresarial no serviço de rede social online e que interagiram de alguma forma com o serviço de rede social online pelo menos uma vez durante o ano, como por exemplo, fazendo login ativamente, abrindo uma página, rolando em uma janela, clicando, curtindo, consultando, postando, comentando ou usando as ferramentas disponíveis para empresas.
Serviços de plataforma de compartilhamento de vídeo	Número de usuários finais únicos que interagiram com o serviço da plataforma de compartilhamento de vídeos pelo menos uma vez durante o mês, por exemplo, reproduzindo um conteúdo audiovisual, fazendo uma consulta ou enviando conteúdo audiovisual, incluindo vídeos gerados pelo usuário.	Número de usuários empresariais únicos que forneceram pelo menos um item de conteúdo audiovisual carregado ou reproduzido no serviço de plataforma de compartilhamento de vídeos durante o ano.
Serviços de comunicações interpessoais independentes de número	Número de usuários finais exclusivos que iniciaram uma comunicação ou participaram de uma comunicação por meio do serviço de comunicações interpessoais independente de número pelo menos uma vez durante o mês.	Número de usuários empresariais exclusivos que usaram uma conta empresarial ou que iniciaram ou participaram de uma comunicação por meio do serviço de comunicações interpessoais independente de número para se comunicar diretamente com um usuário final pelo menos uma vez durante o ano.
Sistemas operacionais	Número de usuários finais exclusivos que usaram um dispositivo com o sistema operacional e o ativaram, atualizaram ou usaram pelo menos uma vez durante o mês.	Número de desenvolvedores únicos que publicaram, atualizaram ou ofereceram pelo menos um aplicativo de computador ou programa de computador que usa a linguagem de programação ou qualquer ferramenta de desenvolvimento do sistema operacional, ou é executado de alguma forma no sistema operacional durante o ano.

Serviços básicos de plataforma	Usuários finais ativos	Usuários profissionais ativos
Assistentes virtuais	Número de usuários finais únicos que interagiram de alguma forma com o assistente virtual pelo menos uma vez durante o mês, por exemplo, ativando-o, fazendo uma pergunta, acessando um serviço por meio de um comando ou controlando um dispositivo de automação residencial.	Número de desenvolvedores exclusivos que, durante o ano, ofereceram pelo menos um aplicativo de computador de assistente virtual ou funcionalidade para tornar um aplicativo de computador existente acessível por meio do assistente virtual.
Navegadores da Web	Número de usuários finais únicos que interagiram com o navegador da web pelo menos uma vez durante o mês, por exemplo, inserindo uma consulta ou um endereço de site na barra de endereços do navegador da web.	Número de usuários empresariais únicos cujos sites empresariais (ou seja, sites usados em caráter comercial ou profissional) foram acessados por meio do navegador da Web pelo menos uma vez durante o ano ou que ofereceram um plug-in, extensão ou complemento usado no navegador da Web durante o ano.
Serviços de computação em nuvem	Número de usuários finais únicos que interagiram com qualquer serviço de computação em nuvem do provedor relevante pelo menos uma vez durante o mês, em troca de qualquer tipo de remuneração, independentemente de tal remuneração ser paga no mesmo mês ou não.	Número de usuários empresariais exclusivos que forneceram qualquer serviço de computação em nuvem hospedado na infraestrutura de nuvem do provedor em questão durante o ano.
Serviços de publicidade online	Para a venda de espaços publicitários próprios: Número de usuários finais exclusivos expostos a uma impressão publicitária pelo menos uma vez durante o mês. Para serviços de intermediação de publicidade (incluindo redes de publicidade, bolsas de publicidade e quaisquer outros serviços de intermediação de publicidade): Número de usuários finais exclusivos expostos pelo menos uma vez durante o mês a uma impressão publicitária que acionou o serviço de corretagem de publicidade.	Para a venda de espaços publicitários próprios: Número de anunciantes exclusivos que veicularam pelo menos uma impressão de anúncio durante o ano. Para serviços de intermediação de publicidade (incluindo redes de publicidade, bolsas de publicidade e quaisquer outros serviços de intermediação de publicidade): Número de usuários empresariais exclusivos (incluindo anunciantes, editores ou outros intermediários) que interagiram ou receberam anúncios do serviço de intermediação de publicidade durante o ano.