



Bruxelas, 26.5.2021
COM(2021) 262 final

**COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO
CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ
DAS REGIÕES**

**Orientações da Comissão Europeia relativas ao reforço do Código de Conduta sobre
Desinformação**

1 INTRODUÇÃO

A crise da COVID-19 ilustrou claramente as ameaças e os desafios que a desinformação coloca às nossas sociedades. A «infodemia» – a rápida disseminação de informações falsas, inexatas ou enganosas sobre a pandemia – criou riscos significativos para a saúde pessoal, os sistemas de saúde pública, a gestão eficaz de crises, a economia e a coesão social. A pandemia aumentou igualmente a importância da tecnologia digital nas nossas vidas, tornando-a cada vez mais central na forma como trabalhamos, aprendemos, socializamos, satisfazemos as necessidades materiais e participamos no discurso cívico. Elevou a fasquia no que diz respeito a garantir que o ecossistema em linha é um espaço seguro e demonstrou que, ainda que os esforços envidados até à data sejam consideráveis, existe uma necessidade premente de os intensificar para combater a desinformação¹.

Desde o seu início², a abordagem da UE em matéria de combate à desinformação baseou-se na proteção da liberdade de expressão e de outros direitos e liberdades garantidos pela Carta dos Direitos Fundamentais da UE. Em consonância com esses direitos e liberdades, em vez de criminalizar ou de proibir a desinformação como tal, a estratégia da UE visa tornar o ambiente em linha e os respetivos intervenientes mais transparentes e responsabilizáveis, dotando as práticas de moderação de conteúdos de maior transparência, capacitando os cidadãos e promovendo um debate democrático aberto³. Para tal, a UE procurou mobilizar todas as partes interessadas, incluindo autoridades públicas, empresas, meios de comunicação, membros da comunidade académica e sociedade civil.

Um elemento central dos esforços da UE foi o código de conduta «autorregulador» sobre desinformação⁴. Os signatários do código – que se encontra em vigor desde outubro de 2018 – incluem agora as principais plataformas em linha ativas na UE, bem como, nomeadamente, grandes associações comerciais que representam o setor europeu da publicidade. A Comissão considera que o código é uma conquista substancial e inédita. Proporcionou um instrumento inovador para assegurar uma maior transparência e responsabilização das plataformas em linha, bem como um quadro estruturado para acompanhar e melhorar as políticas das plataformas em matéria de desinformação.

Todavia, a avaliação do código de conduta realizada em 2020⁵ pela Comissão revelou importantes insuficiências, nomeadamente a aplicação incoerente e incompleta do código nas plataformas e nos Estados-Membros e limitações intrínsecas à natureza «autorreguladora» do código, bem como lacunas na cobertura dos compromissos do código. A avaliação destacou igualmente a falta de um mecanismo de acompanhamento adequado, incluindo indicadores-chave de desempenho (ICD), a falta de compromissos relativos ao acesso aos dados das plataformas para fins de investigação em matéria de desinformação e uma participação limitada das partes interessadas, em especial do setor

¹ Comunicação conjunta «Combater a desinformação sobre a COVID-19: repor a verdade dos factos» [JOIN(2020) 8 final].

² No Plano de Ação contra a Desinformação [JOIN(2018) 36 final], a Comissão Europeia e a Alta Representante estabeleceram uma estratégia abrangente para combater a desinformação na UE.

³ Embora os termos e as condições das plataformas em linha possam abranger igualmente conteúdos que são nocivos, mas não ilegais, quando a desinformação constitui conteúdo ilegal (por exemplo, discursos de ódio ou conteúdos terroristas), são aplicáveis as soluções legislativas pertinentes.

⁴ <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation>.

⁵ SWD(2020) 180 final.

da publicidade. Por conseguinte, a Comissão anunciou, no Plano de Ação para a Democracia Europeia⁶ (EDAP), que emitirá orientações para reforçar o código, como parte de medidas abrangentes destinadas a combater a desinformação no ambiente em linha, e que apresentará legislação específica sobre a transparência da publicidade de cariz político.

A fim de intensificar o combate à desinformação, a proposta de Regulamento Serviços Digitais⁷ (RSD) da Comissão estabelece um quadro de correção por meio de códigos de conduta para dar resposta a riscos sistémicos associados à desinformação. Além disso, introduz medidas de transparência abrangentes no que respeita à moderação de conteúdos e à publicidade e propõe que seja imposta às plataformas em linha de muito grande dimensão⁸ a obrigação jurídica vinculativa e executória de avaliar e dar resposta a riscos sistémicos para os direitos fundamentais ou decorrentes da manipulação intencional do respetivo serviço.

As orientações baseiam-se na experiência da Comissão até à data no que diz respeito ao acompanhamento e à avaliação do código⁹ e no *Report on the 2019 elections to the European Parliament* [relatório da Comissão relativo às eleições de 2019]¹⁰. Contribuem igualmente para a resposta da Comissão às conclusões do Conselho Europeu de dezembro de 2020¹¹. A fim de recolher contributos para as orientações, a Comissão organizou debates entre as várias partes interessadas¹², bem como um seminário para os Estados-Membros.

As presentes orientações expõem os pontos de vista da Comissão sobre a forma como as plataformas e outras partes interessadas devem intensificar as suas medidas para dar resposta a lacunas e a insuficiências do código e criar um ambiente em linha mais transparente, seguro e fiável. Um domínio concreto em que o código não conseguiu realizar progressos suficientes foi a demonetização da desinformação: a publicidade em linha continua a incentivar a divulgação de desinformação¹³. As plataformas em linha e

⁶ COM(2020) 790 final.

⁷ Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Diretiva 2000/31/CE [COM(2020) 825 final]. As referências ao RSD no presente documento devem ser entendidas como referências ao texto proposto pela Comissão.

⁸ A proposta de RSD define as plataformas de muito grande dimensão, no artigo 25.º, como plataformas em linha que prestam os seus serviços a um número médio mensal de destinatários ativos do serviço na União correspondente a 10 % da população da União.

⁹ Avaliação da Comissão de setembro de 2020 [SWD(2020) 180 final].

¹⁰ *Report on the 2019 elections to the European Parliament* [SWD(2020) 113 final], não traduzido para português, disponível em https://ec.europa.eu/info/files/com_2020_252_en.pdf.

¹¹ <https://www.consilium.europa.eu/media/47338/1011-12-20-euco-conclusions-pt.pdf>.

¹² É possível consultar um resumo dos debates com as partes interessadas em: <https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation>.

¹³ Os dados demonstram igualmente que as receitas da publicidade em linha continuam a contribuir significativamente para a monetização dos sítios Web de desinformação, incluindo a publicidade de grandes marcas involuntariamente colocada junto de conteúdos de desinformação (ver, por exemplo, o relatório do Índice Global de Desinformação, em <https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/>, e o relatório da Avaaz, em https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/).

todos os outros intervenientes no ecossistema de publicidade em linha devem, por conseguinte, assumir a responsabilidade e trabalhar em conjunto para cortar o financiamento da desinformação. Além disso, o código revisto deve intensificar os compromissos para limitar o comportamento manipulador, reforçar os instrumentos de capacitação dos utilizadores, aumentar a transparência da publicidade de cariz político e continuar a capacitar a comunidade de investigação e de verificação de factos. As orientações estabelecem igualmente as pedras angulares de um quadro melhorado e sólido para o acompanhamento do código reforçado. O código reforçado deve igualmente visar uma participação mais ampla, com novos signatários, incluindo outras plataformas em linha ativas na UE e outros intervenientes pertinentes.

O reforço do código oferece uma primeira oportunidade para as partes interessadas conceberem medidas adequadas tendo em vista a adoção da proposta de RSD. Em especial, as orientações visam igualmente o desenvolvimento do código de conduta em vigor no sentido do código previsto no artigo 35.º do RSD. As plataformas de muito grande dimensão¹⁴, em particular, beneficiarão da participação no código reforçado, na pendência das novas obrigações que lhes são aplicáveis ao abrigo da proposta de RSD, nomeadamente no que diz respeito à avaliação de riscos, à atenuação de riscos, à capacitação dos utilizadores e à transparência em torno da publicidade. As plataformas de menor dimensão e outras partes interessadas beneficiarão igualmente da subscrição de compromissos adequados no âmbito do código reforçado para tirarem proveito das suas boas práticas e se protegerem contra riscos de reputação decorrentes da utilização abusiva dos seus sistemas para disseminar desinformação.

Sem prejuízo do acordo final entre os legisladores sobre o RSD ou da iniciativa legislativa da Comissão relativa à transparência da publicidade de cariz político, o código de conduta reforçado pode servir de instrumento para ajudar as plataformas em linha a melhorarem as suas políticas e a atenuarem os riscos associados à desinformação que os seus serviços colocam à democracia.

O reforço do código não é unicamente uma etapa transitória. As presentes orientações apelam à transformação do código num instrumento forte, estável e flexível que torne as plataformas em linha mais transparentes, responsabilizáveis e responsáveis desde a conceção.

2 MONITORIZAÇÃO DA COVID-19 – RESULTADOS E ENSINAMENTOS RETIRADOS

Para além dos ensinamentos retirados da avaliação do código de conduta, foram reunidas novas impressões no âmbito do programa de monitorização criado na sequência da Comunicação conjunta «Combater a desinformação sobre a COVID-19: repor a verdade dos factos»¹⁵, durante o qual plataformas em linha signatárias do código comunicaram mensalmente as medidas adotadas para combater a desinformação sobre a COVID-19 na UE.

¹⁴ Na aceção do artigo 25.º do RSD, conforme proposto pela Comissão. Ver a definição na nota de pé de página 8.

¹⁵ Comunicação conjunta «Combater a desinformação sobre a COVID-19: repor a verdade dos factos» [JOIN(2020) 8 final].

O programa de monitorização não só proporcionou uma visão aprofundada das medidas adotadas para combater a desinformação em torno da COVID-19 com base nos compromissos do código, como também submeteu o código a um «teste de esforço».

Os relatórios das plataformas demonstram que os compromissos do código foram aplicados com recurso a medidas eficazes em vários domínios, tais como uma maior visibilidade de fontes fidedignas nos respetivos serviços; o desenvolvimento e a implementação de novos instrumentos e serviços a fim de facilitar o acesso a informações fidedignas; medidas para fazer face a conteúdos que contenham informações falsas ou enganosas suscetíveis de causar danos físicos ou de prejudicar a eficácia das políticas de saúde pública; e a proibição explícita de publicidade que explore a crise ou dissemine desinformação sobre a COVID-19.

A nível geral, o programa demonstrou que o código proporciona um quadro ágil e estruturado, passível de implementação e tradução em medidas decisivas por parte dos signatários para combater a desinformação em situações de crise e que complementa as obrigações previstas nos quadros regulamentares aplicáveis. O código proporcionou igualmente uma estrutura útil para acompanhar estas medidas numa situação excepcional, alterando a ênfase de forma dinâmica à medida que a crise evoluía (por exemplo, a fim de se centrar na desinformação em torno das vacinas contra a COVID-19).

Simultaneamente, o programa relativo à COVID-19 destacou uma série de insuficiências do atual quadro de acompanhamento do código de conduta:

- *qualidade dos relatórios.* Verificam-se variações substanciais em termos de coerência, qualidade e nível de pormenor dos relatórios. A falta de dados com granularidade suficiente, especialmente a nível dos Estados-Membros, fez com que, frequentemente, as informações apresentadas não revelassem se as medidas comunicadas foram aplicadas em todos os Estados-Membros ou em todas as línguas da UE. Além disso, a falta de um modelo de relatório comum e acordado continua a dificultar um acompanhamento mais eficaz e a comparações entre plataformas,
- *ICD.* Embora a qualidade e a granularidade dos relatórios tenham melhorado ao longo do tempo, os dados facultados nem sempre são adequados e suficientemente pormenorizados para avaliar em que medida os compromissos foram aplicados ou qual o efeito das medidas adotadas,
- *avaliação independente.* A monitorização da COVID-19 confirmou a necessidade de uma verificação independente dos relatórios dos signatários, em especial se as políticas e medidas comunicadas foram aplicadas a nível dos Estados-Membros e em todas as línguas da UE e se os relatórios abordam suficientemente as preocupações em matéria de desinformação a nível nacional¹⁶,
- *falta de cobertura suficiente em matéria de verificação de factos.* Durante a «infodemia» de COVID-19, os signatários aumentaram as atividades de verificação de factos nos respetivos serviços, que estão a ser disponibilizadas igualmente a utilizadores de aplicações de mensagens privadas. Todavia, os conteúdos rotulados como falsos por verificadores de factos independentes tendem a voltar a surgir

¹⁶ Conforme previsto na comunicação de junho de 2020, o Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual presta assistência à Comissão no âmbito do programa de monitorização da COVID-19.

noutras plataformas, devido à falta de um repositório centralizado de verificação de factos,

- *monetização contínua da desinformação graças à colocação de anúncios publicitários*. Apesar das medidas que visam limitar a monetização da desinformação, a investigação sobre o tema demonstra que subsistem problemas neste domínio¹⁷.

3 QUESTÕES HORIZONTAIS A ABORDAR

3.1 Compromissos reforçados para atingir os objetivos do código

Os compromissos do atual código de conduta não são suficientemente eficazes para dar uma resposta abrangente aos fenómenos de desinformação. São necessários compromissos mais fortes e mais específicos em todos os domínios do código, a fim de dar resposta às lacunas e às insuficiências, incluindo a riscos novos e emergentes. A fim de assegurar que o código permanece um instrumento vivo, os signatários devem criar um mecanismo permanente para a sua adaptação regular.

3.2 Âmbito alargado

A «infodemia» em torno da pandemia de COVID-19 demonstrou que a informação incorreta¹⁸ (informação falsa ou enganosa disseminada sem intenção maliciosa) também pode prejudicar consideravelmente o interesse público, se se tornar viral. Embora o alvo principal continue a ser a desinformação no sentido estrito do termo¹⁹, no código reforçado os signatários devem comprometer-se a adotar políticas adequadas e medidas proporcionadas para atenuar os riscos colocados pela informação incorreta caso exista uma dimensão significativa de dano público, bem como a prever as devidas garantias de proteção da liberdade de expressão. É necessário capacitar os utilizadores para que possam comparar esta informação com a de fontes fidedignas e informá-los se a informação que estiverem a ver for comprovadamente falsa. Consequentemente, em função da sua natureza, nem todos os compromissos do código se aplicariam à informação incorreta.

A título indicativo, as presentes orientações utilizam o termo «desinformação» como um termo mais abrangente para se referirem aos diferentes fenómenos a que é necessário dar resposta, embora reconheçam claramente a grande diferença existente entre as várias

¹⁷ Um estudo do GDI, de janeiro e fevereiro de 2021, que incidia na França, na Alemanha, na Itália e na Espanha salienta que a maioria das empresas de tecnologia publicitária não possuem políticas específicas em matéria de conteúdos de desinformação sobre a COVID-19 ou as infringem e continuam a financiar sítios Web de notícias publicamente sinalizados como agentes desinformadores: <https://disinformationindex.org/2021/02/ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/>. Um estudo da Avaaz, de agosto de 2020, salientou que os conteúdos dos dez principais sítios Web que disseminam informações incorretas em matéria de saúde tinham quase quatro vezes mais visualizações estimadas no Facebook do que conteúdos equivalentes dos sítios Web das dez principais instituições de saúde: https://secure.avaaz.org/campaign/en/facebook_threat_health/.

¹⁸ O EDAP define informação incorreta do seguinte modo: «Informação incorreta é conteúdo falso ou enganador, partilhado sem intenção de prejudicar mas cujos efeitos podem causar danos, por exemplo quando as pessoas partilham informações falsas com amigos e familiares de boa-fé».

¹⁹ O EDAP define desinformação do seguinte modo: «Desinformação é conteúdo falso ou enganador, disseminado com a intenção de enganar ou de obter um benefício económico ou político e que poderá causar danos públicos».

interpretações²⁰. Desinformação, nesta aceção, inclui a desinformação no sentido estrito do termo, a informação incorreta, bem como as tentativas de exercer influência sobre a informação²¹ e a interferência estrangeira²² no espaço de informação, incluindo por parte de intervenientes externos, casos em que o recurso à manipulação da informação tem por efeito o prejuízo significativo do interesse público.

3.3 Participação alargada

Os signatários do atual código incluem as principais plataformas em linha que operam na UE. Todavia, uma participação mais ampla de plataformas estabelecidas e emergentes poderá permitir dar uma resposta mais abrangente e coordenada à disseminação da desinformação. Os potenciais novos signatários podem incluir prestadores de serviços em linha que divulgam informações ao público, tais como redes sociais de menor dimensão ou serviços de pesquisa (por exemplo, intervenientes que disponibilizam serviços a nível nacional ou regional ou numa base especializada/temática). Dados os encargos de conformidade associados, incluindo as obrigações de apresentação de relatórios, os compromissos assumidos no âmbito do código reforçado devem ter em conta a dimensão dos serviços dos signatários. Embora, de acordo com a proposta de RSD, as plataformas em linha de muito grande dimensão tenham de tomar medidas firmes para dar resposta aos riscos sistémicos pertinentes, as medidas aplicáveis aos serviços de menor dimensão ou emergentes não devem impor-lhes encargos desproporcionados.

Os serviços de mensagens privadas também podem ser utilizados de forma abusiva para alimentar a desinformação e a informação incorreta, conforme se verificou em campanhas eleitorais recentes e durante a pandemia de COVID-19²³. Esses prestadores de serviços poderão ser signatários do código, comprometendo-se a adotar medidas específicas adequadas ao tipo de serviços, sem enfraquecer a encriptação frequentemente utilizada na sua prestação, e tendo em devida conta a proteção da privacidade e o direito à vida privada e familiar, incluindo no que respeita às comunicações.

A fim de aumentar o impacto do código na demonetização da desinformação, é fundamental assegurar uma participação mais ampla das partes interessadas do ecossistema de publicidade, que vá além do círculo dos atuais signatários do código (associações europeias e nacionais do setor da publicidade). O código beneficiaria, em especial, de um maior envolvimento das marcas (em especial das que registam uma despesa considerável com publicidade em linha), bem como de outros participantes do setor da publicidade em linha (por exemplo, bolsas de anúncios, fornecedores de tecnologia publicitária, agências de comunicação) e de outros intervenientes que prestem serviços que possam ser utilizados para monetizar a desinformação (por exemplo,

²⁰ Quando pertinente, as orientações fazem a distinção entre as diferentes subcategorias.

²¹ Tal como definido no EDAP: «Tentativas de exercer influência sobre a informação são esforços coordenados desenvolvidos por intervenientes internos ou externos com o objetivo de influenciar uma audiência-alvo através de vários meios enganadores, incluindo a supressão de fontes de informação independentes em combinação com a desinformação».

²² Tal como definido no EDAP: «*Interferência estrangeira no espaço de informação, realizada frequentemente no âmbito de uma operação híbrida mais vasta, pode ser entendida como esforços desenvolvidos por um interveniente estatal estrangeiro ou pelos seus agentes para corromper a livre formação e expressão da vontade política dos indivíduos, utilizando meios coercivos e enganadores*».

²³ *Stop the virus of disinformation*, Instituto Inter-Regional das Nações Unidas de Investigação sobre o Crime e a Justiça (UNICRI), não traduzido para português, disponível em: <http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf>.

serviços de pagamento eletrónico, plataformas de comércio eletrónico, sistemas de financiamento colaborativo/doação)²⁴.

Os novos signatários poderão incluir igualmente outros intervenientes que possam ter um impacto significativo graças às suas ferramentas, instrumentos, soluções ou conhecimentos específicos pertinentes, incluindo verificadores de factos, organizações que disponibilizam classificações relacionadas com sítios Web de desinformação ou avaliações da desinformação, bem como fornecedores de soluções tecnológicas que possam apoiar os esforços envidados no sentido de combater a desinformação. Tais organizações podem contribuir consideravelmente para uma aplicação eficaz do código e para o seu sucesso.

3.4 Compromissos específicos

A fim de facilitar uma participação mais ampla, o código reforçado deve incluir compromissos específicos que correspondam à diversidade de serviços prestados pelos signatários e às funções específicas que desempenham no ecossistema.

Os signatários devem subscrever os compromissos pertinentes para os seus serviços. Embora a participação no código e a subscrição dos respetivos compromissos continue a ser voluntária, de modo a assegurar a eficácia do código enquanto instrumento de atenuação de riscos, os signatários não devem, em princípio, poder optar por não subscrever compromissos aplicáveis aos seus serviços. Caso os signatários optem por não subscrever um determinado compromisso aplicável aos seus serviços, devem apresentar uma justificação pública, em conformidade com o espírito do considerando 68 da proposta de RSD. Os signatários que disponibilizem ferramentas, instrumentos ou soluções para combater a desinformação poderão subscrever os compromissos adequados e utilizar os seus conhecimentos especializados para apoiar outros signatários do código. Quaisquer requisitos de apresentação de relatórios impostos a essas organizações devem ser adaptados à sua missão.

3.5 Observatório Europeu dos Meios de Comunicação Digitais

A fim de contribuir eficazmente para resolver o problema da desinformação, é essencial contar com o apoio de uma comunidade multidisciplinar, incluindo verificadores de factos, investigadores académicos e outras partes interessadas. De modo a contribuir para a criação dessa comunidade e facilitar o seu trabalho, foi criado o Observatório Europeu dos Meios de Comunicação Digitais (EDMO)²⁵. Ao prestar apoio a verificadores de factos e investigadores independentes, o EDMO e os respetivos centros nacionais aumentarão a sua capacidade de deteção e análise de campanhas de desinformação. O EDMO pode desempenhar um papel importante na consecução de vários objetivos do código. Por conseguinte, é de esperar que os signatários do código, quando necessário, cooperem com o EDMO.

²⁴ *How COVID-19 conspiracists and extremists use crowdfunding platforms to fund their activities*, EU DisinfoLab, disponível em <https://www.disinfo.eu/publications/how-covid-19-conspiracists-and-extremists-use-crowdfunding-platforms-to-fund-their-activities/>.

²⁵ <https://edmo.eu/>.

3.6 Sistema de alerta rápido

Tal como delineado no Plano de Ação contra a Desinformação de 2018²⁶, as plataformas em linha devem cooperar com o sistema de alerta rápido da UE, que liga todos os Estados-Membros da UE e as instituições pertinentes da UE, a fim de permitir dar respostas conjuntas à desinformação, mediante um intercâmbio de informações e um fornecimento imediato de alertas para o lançamento de campanhas de desinformação. Deste modo, o código reforçado deve explorar oportunidades para consolidar essa cooperação, nomeadamente facilitando um intercâmbio informal entre os signatários a fim de apresentarem o seu trabalho e as suas conclusões, bem como para assegurar ligações estreitas, racionalizadas e coerentes a nível nacional entre todos os Estados-Membros e os signatários, conforme adequado. Tal deve ter igualmente em conta a cooperação com o EDMO, como mencionado anteriormente.

4 CONTROLO DA COLOCAÇÃO DE ANÚNCIOS

Conforme explicado, para que o código seja bem-sucedido, são fundamentais medidas decisivas que visem demonetizar os agentes desinformadores. Os compromissos do código reforçado devem, por conseguinte, prever medidas mais granulares e adaptadas, a fim de dar resposta aos riscos da desinformação associados à distribuição de publicidade em linha, tendo em mente os futuros requisitos regulamentares da proposta de RSD aplicáveis a toda a publicidade em linha, incluindo a publicidade de cariz político e a publicidade temática, e, se aplicável, a iniciativa anunciada relativa à publicidade de cariz político.

4.1 Demonetização da desinformação

O código deve reforçar os compromissos que visam cortar o financiamento à divulgação de desinformação nos próprios serviços dos signatários ou em sítios Web de terceiros²⁷. A fim de melhorar a transparência e a responsabilização no que se refere à colocação de anúncios, os signatários que participam nesta atividade, incluindo as empresas de tecnologia publicitária²⁸, devem identificar os critérios que utilizam para colocar anúncios e adotar medidas que permitam a verificação do local de destino dos anúncios, com o objetivo de evitar que sejam colocados junto a conteúdos de desinformação ou em locais conhecidos pela publicação repetida de desinformação. As plataformas devem comprometer-se, em especial, a reforçar os requisitos de elegibilidade e os processos de revisão de conteúdos para programas de partilha de receitas publicitárias e monetização de conteúdos nos seus serviços, de modo a proibir a participação de intervenientes que publiquem sistematicamente conteúdos desmentidos²⁹. Além disso, as plataformas devem comprometer-se igualmente a reforçar as políticas pertinentes e a exercer as devidas

²⁶ JOIN(2018) 36 final.

²⁷ Os dados demonstram igualmente que as receitas da publicidade em linha continuam a contribuir significativamente para a monetização dos sítios Web de desinformação, incluindo a publicidade de grandes marcas involuntariamente colocada junto de conteúdos de desinformação. Por exemplo, o Índice Global de Desinformação estima que, anualmente, cerca de 76 milhões de USD em receitas publicitárias revertam para sítios Web de desinformação que têm a Europa como alvo:

<https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/>.

²⁸ Um número limitado de empresas de tecnologia publicitária já adotou essas políticas.

²⁹ Ver, por exemplo, o relatório de 2020 da Avaaz, *Why is YouTube Broadcasting Climate Misinformation to Millions?*, não traduzido para português, disponível em:

https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/.

diligências, com vista a excluir a participação, nas redes publicitárias ou bolsas de anúncios, de sítios Web que facultem persistentemente conteúdos de desinformação.

Os compromissos neste domínio devem igualmente basear-se na disponibilidade e na adoção de instrumentos de segurança das marcas e melhorá-los. Estes instrumentos devem integrar informações e análises de verificadores de factos, investigadores e outras partes interessadas que facultem informações, por exemplo, relativas às fontes de campanhas de desinformação. Com o apoio dessas informações e instrumentos, os proprietários de marcas e outros anunciantes devem comprometer-se a envidar todos os esforços para evitar a colocação dos seus anúncios junto a conteúdos de desinformação ou em locais que reiteradamente publiquem desinformação.

4.2 Melhoria da cooperação entre os intervenientes pertinentes

A obtenção de resultados tangíveis requer a estreita cooperação de diferentes intervenientes no ecossistema de publicidade. Para tal, conforme exposto na secção 3.3, é fundamental uma participação mais ampla das partes interessadas do ecossistema de publicidade. O código reforçado deve proporcionar um enquadramento para essa participação alargada, ao consolidar a cooperação de todos os intervenientes pertinentes e ao facilitar ainda mais as iniciativas intersetoriais em curso neste domínio³⁰.

No âmbito do código reforçado, todos os intervenientes envolvidos na compra, na venda e na colocação de publicidade digital devem comprometer-se a partilhar as melhores práticas e a reforçar a cooperação. Essa cooperação deve facilitar a integração e a circulação de informações ao longo de toda a cadeia de valor publicitária, em especial informações pertinentes para a identificação dos agentes desinformadores, no pleno respeito de todas as regras aplicáveis em matéria de proteção de dados.

A cooperação entre plataformas poderá incluir igualmente o intercâmbio de informações relativas a anúncios de desinformação recusados por uma plataforma, a fim de impedir o seu aparecimento noutras plataformas – por exemplo, através da criação de um repositório comum de anúncios recusados –, para que outras plataformas cujos serviços possam igualmente ser afetados tomem conhecimento.

A participação de intervenientes ativos na cadeia de valor da monetização em linha, tais como serviços de pagamento eletrónico em linha, plataformas de comércio eletrónico e sistemas pertinentes de financiamento colaborativo/doação, deverá permitir alargar as ações que visam cortar o financiamento à desinformação.

³⁰ A *Global Alliance for Responsible Media* [Aliança mundial para meios de comunicação responsáveis], lançada em junho de 2019 sob os auspícios da Federação Mundial de Anunciantes (FMA), inclui plataformas e signatários do código do setor da publicidade, bem como outras partes interessadas importantes de todo o ecossistema de publicidade. Está a desenvolver um conjunto de definições e normas comuns a todo o setor quanto à forma como os conteúdos nocivos são categorizados nas plataformas. Estas definições e normas são aprovadas pelos anunciantes e aplicadas pelas plataformas aos seus produtos publicitários e instrumentos de segurança das marcas. A Aliança pretende, nomeadamente, incluir nesse conjunto uma categoria distinta para a desinformação e a informação incorreta. Ver *Interim Report on Activities related to the EU Code of Practice on Disinformation*, da FMA, de setembro de 2020, p. 2, não traduzido para português, disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69683

4.3 Compromissos para combater a publicidade que contém desinformação

Nos termos do código reforçado, os signatários devem comprometer-se a conceber políticas adequadas e adaptadas em matéria de publicidade, que combatam a utilização abusiva dos seus sistemas de publicidade para a propagação de desinformação³¹. Devem fazer cumprir estas políticas de forma coerente e eficaz. Para tal, os signatários devem cooperar com os verificadores de factos a fim de identificar anúncios que contenham desinformação que tenha sido verificada e denunciada. De modo a assegurar uma aplicação coerente, os signatários devem comprometer-se a adaptar os seus atuais sistemas de verificação e revisão de anúncios para garantir que os anúncios colocados nos seus serviços, ou através dos mesmos, cumprem as suas políticas publicitárias no que diz respeito à desinformação. Os signatários devem igualmente comprometer-se a explicar claramente aos anunciantes quais as políticas publicitárias violadas quando rejeitarem ou removerem anúncios de desinformação ou desativarem contas de publicidade³².

5 PUBLICIDADE DE CARIZ POLÍTICO E PUBLICIDADE TEMÁTICA

A «publicidade de cariz político» e a «publicidade temática»³³ desempenham um papel importante na organização de campanhas políticas e de debates públicos em torno de questões societais fundamentais. Estes conteúdos pagos em linha podem ter um papel decisivo na formação da opinião pública e influenciar os resultados eleitorais. A organização de eleições na UE encontra-se amplamente regulamentada a nível dos Estados-Membros. São várias as regras aplicáveis que afetam a publicidade de cariz político, incluindo a sua transparência. No EDAP, a Comissão anunciou legislação que visa reforçar a transparência da publicidade de cariz político. A fim de assegurar o nível adequado de transparência e de responsabilização neste domínio, os compromissos do código carecem de um reforço adicional, que apoie o quadro jurídico mais amplo.

A revisão do código neste domínio terá de ter em conta a futura proposta legislativa da Comissão relativa à transparência dos conteúdos políticos patrocinados e as disposições pertinentes da proposta de RSD. Um código reforçado constituirá um veículo importante para proporcionar progressos tangíveis que apoiem o atual quadro jurídico, para abrir caminho a uma legislação reforçada e através do novo quadro legislativo uma vez adotado, bem como para conceber soluções orientadas para o setor, com vista a apoiar a sua aplicação e a alcançar progressos contínuos neste domínio.

Para uma execução coerente e eficaz dos compromissos, é necessário um entendimento comum dos conceitos de «publicidade de cariz político» e «publicidade temática» por parte dos signatários, que tenha devidamente em conta os quadros jurídicos nacionais aplicáveis em vigor. Os signatários devem certificar-se de que cumprem a legislação

³¹ Os dados demonstram a persistência em linha de anúncios que contêm desinformação, mesmo após a sua identificação e denúncia por parte dos verificadores de factos. Ver *Facebook Approved Ads With Coronavirus Misinformation*: <https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/>.

³² Conforme observado pela Comissão, as políticas das plataformas prosseguem diversos objetivos, sendo que alguns não são especificamente adaptados ao combate à desinformação (por exemplo, alegações comerciais sem fundamentação e práticas comerciais enganosas). Ver SWD(2020) 180 final.

³³ Embora o código não contenha atualmente uma definição comum de publicidade temática, parece haver consenso quanto ao facto de que se trata de publicidade que inclui conteúdos patrocinados relativos a questões societais ou ligadas a um debate de interesse geral que pode influenciar o discurso público. São exemplos destas questões as alterações climáticas, questões ambientais, a imigração ou a COVID-19.

aplicável e harmonizar as suas práticas com a futura legislação sobre a transparência dos conteúdos políticos patrocinados.

5.1 Rotulagem eficaz da publicidade de cariz político e da publicidade temática

O código deve incluir compromissos reforçados que assegurem a transparência e a divulgação pública da publicidade de cariz político e da publicidade temática, tendo em conta as disposições pertinentes da proposta de RSD³⁴, a futura iniciativa legislativa sobre a transparência da publicidade de cariz político e sem prejuízo dos quadros regulamentares em vigor. Esta publicidade deve estar rotulada e ser reconhecível, de forma clara e eficaz, como conteúdo pago e os utilizadores devem ser capazes de compreender que o conteúdo apresentado contém publicidade relacionada com questões políticas ou societárias. O código reforçado poderá incluir um conjunto de critérios e exemplos comuns relativos à identificação e à rotulagem da publicidade de cariz político e da publicidade temática. Quando pertinente, os signatários devem integrar resultados de investigações pertinentes, a fim de melhorar a eficácia dos rótulos em termos de informação dos utilizadores³⁵. O código deve incluir compromissos que visem assegurar que os rótulos permanecem ativos quando os utilizadores partilham publicidade de cariz político e publicidade temática de forma orgânica³⁶, de modo a continuarem a ser claramente identificadas como publicidade.

5.2 Compromissos em matéria de verificação e de transparência da publicidade de cariz político e da publicidade temática

Os signatários que apresentam publicidade de cariz político e publicidade temática devem assegurar que a identidade do anunciante é visível para os utilizadores, incluindo um compromisso específico que estabeleça obrigações em matéria de transparência em conformidade com os requisitos da proposta de RSD³⁷.

Os signatários devem igualmente envidar esforços razoáveis para garantir, através de sistemas eficazes de verificação da identidade e de autorização, que estão cumpridas todas as condições necessárias antes de autorizarem a colocação deste tipo de anúncios.

5.3 Transparência nas plataformas de mensagens

O código de conduta revisto deve incluir compromissos novos e específicos que deem resposta à utilização de plataformas de mensagens para divulgar publicidade de cariz político e publicidade temática, no pleno respeito do Regulamento Geral sobre a Proteção de Dados (RGPD) e dos requisitos da UE em matéria de privacidade nos serviços de comunicações eletrónicas. O requisito supramencionado de que os conteúdos políticos patrocinados permaneçam rotulados como conteúdos pagos quando são partilhados entre utilizadores deve aplicar-se igualmente, na medida do possível, aos conteúdos políticos patrocinados partilhados em plataformas de mensagens. Para tal, os signatários devem

³⁴ Em especial, o artigo 24.º.

³⁵ Dobber *et al.*, *Effectiveness of online political ad disclosure labels: empirical findings*, de março de 2021, não traduzido para português, disponível em: <https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-disclosures-experiment-update.pdf>.

³⁶ Os conteúdos orgânicos são conteúdos gratuitos que os utilizadores partilham entre si sem pagar. Incluem também as situações em que os utilizadores partilham entre si conteúdos patrocinados que depois se tornam conteúdos orgânicos.

³⁷ Artigo 30.º da proposta de RSD.

desenvolver soluções compatíveis com a tecnologia de encriptação frequentemente utilizada pelas plataformas de mensagens, sem enfraquecerem a encriptação.

5.4 Direcionamento de publicidade de cariz político

O microdirecionamento de publicidade de cariz político pode suscitar várias preocupações. Pode levantar questões de conformidade com as regras em matéria de proteção de dados, uma vez que se baseia em informações pessoais e, por vezes, inclui técnicas sofisticadas da chamada perfilagem psicológica³⁸. Pode afetar o direito dos eleitores a receberem informação, uma vez que permite aos anunciantes políticos enviarem mensagens personalizadas para públicos-alvo, enquanto outros públicos podem ser privados destas informações. O microdirecionamento dificulta a verificação ou o controlo dessa publicidade, bem como a possibilidade de as pessoas fazerem valer os seus direitos, incluindo em matéria de proteção de dados, o que, por sua vez, pode aumentar o risco de polarização política³⁹.

O código reforçado deve contribuir para limitar ou evitar os riscos associados ao microdirecionamento de publicidade de cariz político e/ou temática para pessoas singulares. A este respeito, deve ser assegurada a plena conformidade com o RGPD e outra legislação pertinente, em especial no que diz respeito à obtenção de consentimento válido sempre que necessário⁴⁰. Deve ser facilitado o acesso à informação, de modo que as autoridades competentes possam desempenhar as suas funções de controlo e de execução.

Os signatários devem comprometer-se a assegurar que os cidadãos são claramente informados quando são alvo de microdirecionamento e que lhes são facultadas informações úteis relativas aos critérios e aos dados utilizados para o efeito. Devem aplicar fortes medidas de transparência neste domínio, incluindo bibliotecas de anúncios dedicadas e consultáveis, que incluam todos os anúncios microdirecionados apresentados a grupos específicos de utilizadores⁴¹, acompanhadas de informações sobre os critérios de direcionamento e de publicação.

5.5 Melhoria dos repositórios de anúncios e das funcionalidades mínimas das interfaces de programação de aplicações (IPA)

O código reforçado deve assegurar que as plataformas signatárias se comprometem a melhorar a exaustividade e a qualidade das informações constantes dos seus repositórios de publicidade de cariz político, para que incluam efetivamente todos os conteúdos políticos patrocinados apresentados. Estes repositórios devem facultar informações atuais

³⁸ A proposta de RSD e a proposta de regulamento relativo aos mercados digitais preveem obrigações específicas em matéria de transparência.

³⁹ Ver, por exemplo, Papakryiakopoulos *et al.*, *Social media and microtargeting: Political data processing and the consequences for Germany*, Big Data & Society, de novembro de 2018, DOI 10.1177/2053951718811844, ou Lewandowsky *et al.*, *Understanding the influence of online technologies on political behaviour and decision-making*, EUR 30422 EN, Serviço das Publicações da União Europeia, Luxemburgo, não traduzidos para português.

⁴⁰ Para mais orientações, ver [Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679](#) e [Guidelines 08/2020 on the targeting of social media users](#), não traduzido para português (que apresentam exemplos de casos em que é necessário consentimento para o direcionamento de publicidade), do Comité Europeu para a Proteção de Dados.

⁴¹ Por exemplo, as bibliotecas de anúncios, se contiverem os dados necessários, podem ser utilizadas para verificar se existe a mesma exposição temporal em linha a mensagens políticas.

e regularmente atualizadas sobre o volume e o orçamento da publicidade de cariz político apresentada por anunciantes políticos nos Estados-Membros, o número de vezes que cada anúncio foi apresentado em linha e os critérios de direcionamento utilizados pelo anunciante, tendo em conta as disposições aplicáveis da proposta de RSD e a futura proposta legislativa relativa à publicidade de cariz político⁴².

Algumas plataformas desenvolveram interfaces de programação de aplicações (IPA) ou outras que permitem aos utilizadores e investigadores efetuarem pesquisas personalizadas nos seus repositórios de publicidade de cariz político. Todavia, as funcionalidades destas IPA são muito limitadas. O código reforçado deve assegurar que as IPA dos repositórios de publicidade de cariz político das plataformas incluem um conjunto de funcionalidades mínimas, bem como um conjunto de critérios mínimos de pesquisa que permitam aos utilizadores e aos investigadores efetuar pesquisas personalizadas, a fim de obter dados em tempo real em formatos normalizados, e facilitem a comparação, a pesquisa e o acompanhamento entre plataformas. Se forem criados repositórios para publicidade temática, estes devem possuir funcionalidades de IPA e capacidades de pesquisa equiparáveis. Os compromissos devem assegurar igualmente um amplo acesso às IPA e que as funcionalidades das IPA são regularmente atualizadas a fim de satisfazer as necessidades dos investigadores.

6 INTEGRIDADE DOS SERVIÇOS

O código reforçado deve prever uma cobertura abrangente das formas atuais e emergentes de comportamento manipulador utilizadas para disseminar desinformação. Deve ter em conta a natureza evolutiva da desinformação e os riscos mais vastos associados à disseminação da desinformação, por exemplo, o facto de as campanhas de desinformação poderem fazer parte de ameaças híbridas à segurança, nomeadamente em combinação com ciberataques⁴³. Deve incluir compromissos específicos para dar resposta às vulnerabilidades e assegurar a transparência e a responsabilização no respeitante às medidas tomadas pelos signatários para limitar comportamentos manipuladores, que, de acordo com as suas condições de utilização, não são permitidos nos serviços dos signatários, tendo igualmente em conta os futuros requisitos regulamentares estabelecidos na proposta de RSD⁴⁴.

6.1 Entendimento comum de comportamento manipulador inadmissível

A fim de assegurar uma abordagem coerente, o código reforçado deve garantir que os signatários chegam a acordo sobre um entendimento interserviços dos comportamentos manipuladores não permitidos nos seus serviços, incluindo dos «comportamentos inautênticos», sem prejuízo da legislação nacional e da UE em vigor. Esse entendimento deve ser suficientemente amplo para abranger todo o leque de comportamentos com que os agentes mal-intencionados possam tentar manipular os serviços. Para o efeito, os signatários devem elaborar uma lista abrangente de táticas, técnicas e procedimentos de manipulação que constituem comportamentos inautênticos inadmissíveis nos seus serviços. As técnicas identificadas devem estar suficientemente definidas para permitir a

⁴² Ver artigo 30.º da proposta de RSD.

⁴³ Comunicação Conjunta intitulada «Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas [JOIN(2018) 16 final].

⁴⁴ O artigo 26.º, n.º 1, alínea c), da proposta de RSD identifica «manipulação intencional» de serviços como um risco sistémico, contra o qual as plataformas de muito grande dimensão devem tomar medidas de atenuação de riscos.

comparação da prevalência de comportamentos inadmissíveis entre plataformas, bem como a eficácia das medidas tomadas para os combater. O entendimento comum deve facultar aos signatários, reguladores, sociedade civil e outras partes interessadas um léxico comum que lhes permita discutir problemas de desinformação e manipulação em linha, tanto no contexto do código de conduta como noutras instâncias, como o sistema de alerta rápido da UE e a rede europeia de cooperação para as eleições, e tendo em vista a execução da proposta de RSD. Este trabalho deve ter em conta a rápida evolução da situação no que diz respeito às táticas, técnicas e procedimentos e refletir essas eventuais alterações aquando da elaboração da terminologia e das definições.

6.2 Compromissos reforçados para limitar os comportamentos manipuladores inadmissíveis

O código reforçado deve estabelecer novos compromissos relativos aos comportamentos manipuladores inadmissíveis, que abranjam todo o leque de técnicas de manipulação e exijam respostas eficazes para as combater. Os compromissos devem exigir que os signatários deem resposta a técnicas de manipulação em evolução, tais como operações de pirataria com vista à obtenção e divulgação de informações, apropriação de contas, criação de grupos inautênticos, usurpação de identidade, falsificações profundas, compra de interações falsas ou o envolvimento opaco de influenciadores. Além disso, os compromissos devem não só exigir que os signatários publiquem políticas pertinentes, mas também estabelecer elementos de base, objetivos e critérios de referência para as medidas implementadas para combater os comportamentos manipuladores inadmissíveis. O código reforçado deve ter em consideração as obrigações de transparência para os sistemas de IA que geram ou manipulam conteúdos e a lista de práticas de manipulação proibidas pela proposta de Regulamento Inteligência Artificial⁴⁵.

6.3 Adaptação dos compromissos, cooperação e transparência

A fim de assegurar a sua contínua relevância e adequação, o código reforçado deve criar um mecanismo através do qual os respetivos compromissos possam ser adaptados ao longo do tempo, com base nos dados mais recentes relativos às condutas e às táticas, técnicas e procedimentos utilizados por agentes mal-intencionados.

Os signatários devem comprometer-se a criar canais de intercâmbio informações entre as respetivas equipas de cibersegurança, segurança e confiança. Estes canais de intercâmbio devem facilitar a partilha pró-ativa de informações sobre as tentativas de exercer influência e a interferência estrangeira no espaço de informação dos serviços dos signatários, a fim de impedir que essas campanhas voltem a surgir noutras plataformas. Os resultados e os ensinamentos retirados devem ser incluídos nos relatórios anuais de acompanhamento dos signatários, debatidos no grupo de trabalho permanente⁴⁶ e disponibilizados regularmente em formatos comuns de dados⁴⁷.

Os compromissos devem assegurar que todas as políticas e medidas são claramente comunicadas aos utilizadores, incluindo por intermédio do centro de transparência⁴⁸. Os

⁴⁵ COM(2021) 206 final.

⁴⁶ A respeito do grupo de trabalho permanente, ver a secção 9.2.3 *infra*.

⁴⁷ Estes formatos devem ter igualmente em conta o quadro AMITT [do inglês «Adversarial Misinformation and Influence Tactics and Techniques» (Táticas e técnicas antagonistas de informação incorreta e influência)]: <https://cogsec-collab.org/>.

⁴⁸ No que respeita ao centro de transparência, ver a secção 9.2.2 *infra*.

signatários devem comprometer-se igualmente a submeter todas as medidas contra comportamentos manipuladores inadmissíveis a um sistema interno de tratamento de reclamações, tendo em consideração as disposições pertinentes da proposta de RSD⁴⁹.

7 CAPACITAÇÃO DOS UTILIZADORES

A fim de limitar o impacto da desinformação, é fundamental capacitar os utilizadores. Uma melhor compreensão do funcionamento dos serviços em linha, bem como a disponibilização de instrumentos que promovam um comportamento mais responsável em linha ou que permitam aos utilizadores detetar e denunciar conteúdos falsos e/ou enganosos, podem limitar significativamente a disseminação da desinformação. Os compromissos do código neste domínio devem ser alargados, de modo a abranger um vasto leque de serviços, incluindo, por exemplo, compromissos específicos para os serviços de mensagens. Devem incluir igualmente mecanismos de recurso contra medidas tomadas pelos signatários para dar seguimento às comunicações dos utilizadores. Os signatários devem também ter especificamente em conta a situação das crianças, que podem ser particularmente vulneráveis à desinformação.

7.1 Compromisso em prol de medidas de reforço da literacia mediática

Vários signatários envidaram esforços no domínio da literacia mediática, disponibilizando aos utilizadores instrumentos pertinentes. No âmbito do código reforçado, os signatários devem comprometer-se a prosseguir estes esforços e, em particular, a envolver de forma mais ativa a comunidade de literacia mediática na conceção e aplicação de instrumentos e na avaliação de campanhas de literacia mediática dos respetivos serviços, nomeadamente para proteger as crianças. A fim de explorar sinergias pertinentes, estes esforços poderão igualmente ser harmonizados com as iniciativas da Comissão no domínio da literacia mediática⁵⁰, incluindo o novo Plano de Ação para a Educação Digital (2021-2027)⁵¹. Para tal, o grupo de peritos da Comissão em matéria de literacia mediática⁵² e o EDMO podem ajudar a estabelecer um quadro permanente de debate.

7.2 Compromisso em prol da «conceção segura»

A conceção e a arquitetura dos serviços em linha têm um impacto significativo no comportamento dos utilizadores⁵³. Por conseguinte, os signatários devem comprometer-se a avaliar os riscos colocados pelos seus sistemas e a conceber a arquitetura dos seus serviços de forma a minimizar os riscos associados⁵⁴ à disseminação e à amplificação da

⁴⁹ Nomeadamente o artigo 17.º, que já é aplicável a decisões incompatíveis com os seus termos e condições, incluindo as decisões de remover ou desativar o acesso aos conteúdos, as decisões de suspender ou cessar parcial ou integralmente a prestação do serviço ao destinatário ou as decisões de suspender ou encerrar a conta do destinatário.

⁵⁰ Ver, em particular, as medidas estabelecidas no Plano de Ação para a Democracia Europeia, [COM(2020) 790 final] e no Plano de Ação para os Meios de Comunicação Social e o Setor Audiovisual [COM(2020) 784 final].

⁵¹ O Plano de Ação para a Educação Digital [COM(2020) 624 final] propõe o desenvolvimento de orientações para os professores e educadores, com vista a combater a desinformação e promover a literacia digital através da educação e da formação.

⁵² <https://digital-strategy.ec.europa.eu/en/policies/media-literacy>.

⁵³ Ver, por exemplo, Lewandowsky *et al.*, *Understanding the influence of online technologies on political behaviour and decision-making*, EUR 30422 EN, Serviço das Publicações da União Europeia, Luxemburgo, 2020, não traduzido para português.

⁵⁴ Ver artigo 26.º, n.º 1, alínea c), da proposta de RSD, relativo à avaliação de riscos conexa.

desinformação⁵⁵, nomeadamente efetuando testes prévios à arquitetura dos sistemas. Os signatários devem também investir em investigação e desenvolver funcionalidades e desenhos de produtos que favoreçam o espírito crítico dos utilizadores, bem como a utilização responsável e segura dos seus serviços.

As plataformas em linha poderão igualmente colaborar com os fornecedores de soluções tecnológicas, a fim de integrar nos seus serviços soluções que permitam verificar a autenticidade ou a exatidão, ou identificar a proveniência ou a fonte de conteúdos digitais⁵⁶.

Os fornecedores de sistemas em linha baseados em IA devem ter igualmente em consideração as disposições pertinentes da proposta de Regulamento Inteligência Artificial.

7.3 Responsabilização dos sistemas de recomendação

Ao determinarem a ordem pela qual a informação é apresentada, os sistemas de recomendação têm um impacto significativo nas informações a que os utilizadores efetivamente acedem. É da máxima importância que, no âmbito do código reforçado, os signatários se comprometam a tornar os seus sistemas de recomendação transparentes no que diz respeito aos critérios utilizados para atribuir ou retirar prioridade à informação, dando aos utilizadores a possibilidade de personalizarem os algoritmos de classificação. Tudo isto deve ser feito no devido respeito pelo princípio da liberdade dos meios de comunicação social, tendo em conta os requisitos das disposições pertinentes da proposta de RSD⁵⁷.

Os compromissos devem também incluir medidas concretas para atenuar os riscos de os sistemas de recomendação alimentarem a disseminação viral de desinformação, nomeadamente a exclusão de informações falsas e/ou enganosas dos conteúdos recomendados quando tiverem sido desmentidas por verificadores de factos independentes e a exclusão de páginas Web e de intervenientes que disseminem desinformação de forma persistente.

7.4 Visibilidade de informações fidedignas de interesse público

A pandemia de COVID-19 salientou a importância, especialmente em tempos de crise, de promover informações de interesse público que sejam fidedignas, como informações relativas a medidas de prevenção da doença ou à segurança das vacinas facultadas pelas

⁵⁵ Algumas intervenções técnicas simples (por exemplo, mensagens instantâneas que perguntem aos utilizadores se pretendem realmente partilhar ligações que não visualizaram) podem incitar os utilizadores a analisarem os conteúdos antes de os divulgarem e, desse modo, ajudar a limitar a disseminação de informações falsas e/ou enganosas por parte de utilizadores que ajam de boa-fé. Exemplos: o alerta «Leia antes de Tweetar» implementado pelo Twitter: <https://help.twitter.com/pt/using-twitter/how-to-retweet>; os painéis de informações verificadas do YouTube: <https://support.google.com/youtube/answer/9229632?hl=pt>; o aviso instantâneo do Facebook apresentado antes da partilha de conteúdos desmentidos por um verificador de factos: <https://www.facebook.com/journalismproject/programs/third-party-fact-checking/faqs>; o «Know your facts tool» do TikTok [Instrumento conheça os factos]: <https://newsroom.tiktok.com/en-gb/taking-action-against-covid-19-vaccine-misinformation>.

⁵⁶ Na secção 3.3, as orientações convidam as partes interessadas que possam contribuir para o combate à desinformação com as suas ferramentas, instrumentos, ou soluções a tornarem-se novos signatários do código.

⁵⁷ Nomeadamente, os artigos 26.º, 27.º e 29.º.

autoridades de saúde⁵⁸. Os signatários implementaram várias soluções para facultarem essas informações aos utilizadores e as tornarem visíveis e de fácil acesso. Com base nesta experiência, os signatários do código reforçado devem comprometer-se a continuar a desenvolver e aplicar instrumentos específicos (por exemplo, painéis informativos, faixas, janelas instantâneas, mapas e alertas) que atribuam prioridade e direcionem os utilizadores para fontes fidedignas no que respeita a assuntos de especial interesse público e societal ou em situações de crise.

A fim de aprofundar o compromisso⁵⁹ do atual código de dar prioridade a conteúdos pertinentes, autênticos e fidedignos, os signatários devem também comprometer-se a publicar uma descrição da metodologia utilizada pelos seus sistemas de recomendação para esse fim. Estas informações devem figurar no centro de transparência. Os signatários do código devem estudar a possibilidade de garantir que estas informações possam ser verificadas por terceiros ou mediante uma auditoria independente, tendo igualmente em consideração as disposições pertinentes da proposta de RSD.

7.5 Emissão de avisos dirigidos aos utilizadores que interagem ou interagiram com conteúdos falsos ou enganosos

Desmentir informações falsas e/ou enganosas é fundamental para travar os fenómenos de desinformação⁶⁰. Vários signatários estabeleceram relações de colaboração com verificadores de factos independentes e/ou criaram equipas internas de moderação, a fim de disponibilizar rótulos para conteúdos falsos ou enganosos. Todavia, atualmente, o código não inclui compromissos nesta matéria. Deste modo – complementando os novos compromissos destinados a assegurar a execução coerente da verificação de factos, tal como abordado na secção 8.3 *infra* –, os signatários devem comprometer-se a disponibilizar, em todas as línguas da UE nas quais o seu serviço é prestado, sistemas para a rotulagem regular e coerente de conteúdos identificados como falsos ou enganosos e para a emissão de avisos dirigidos aos utilizadores que interagiram com os mesmos. Os signatários devem comprometer-se a informar os utilizadores sobre os motivos pelos quais determinados conteúdos ou contas foram rotulados, despromovidos ou de qualquer outro modo afetados por medidas tomadas, bem como sobre o fundamento dessa ação. Os signatários devem comprometer-se a conceber os seus sistemas de rotulagem e de aviso com base em dados científicos atualizados sobre a forma de maximizar o impacto dessas intervenções, assegurando, em especial, que são concebidos de modo a captar a atenção dos utilizadores⁶¹.

7.6 Funcionalidade para sinalizar informações falsas e prejudiciais

Embora alguns signatários já disponibilizem aos utilizadores uma funcionalidade específica para sinalização de informações falsas e/ou enganosas, esta ainda não está disponível em todos os serviços. O código reforçado deve incluir um compromisso específico que exija que os signatários disponibilizem procedimentos fáceis e eficazes

⁵⁸ Os relatórios de monitorização da COVID-19 fornecem dados relativos às visualizações ou às taxas de cliques das faixas e painéis informativos que facultam essas informações: <https://digital-strategy.ec.europa.eu/en/library/reports-march-actions-fighting-covid-19-disinformation-monitoring-programme>.

⁵⁹ Ver compromisso 8 do Código de Conduta sobre Desinformação.

⁶⁰ O Manual da Desmistificação 2020, disponível em: <https://sks.to/db2020>.

⁶¹ É possível otimizar, por exemplo, a conceção visual e o momento ou a apresentação gráfica da intervenção.

nos seus serviços, que permitam aos utilizadores sinalizar a desinformação com potencial para causar danos públicos ou pessoais. Esta funcionalidade deve igualmente apoiar os sistemas e os mecanismos de rotulagem, a fim de ajudar a identificar conteúdos com informações falsas que voltem a surgir e que já tenham sido rotulados como falsos noutras línguas ou noutros serviços, no pleno respeito pela liberdade de expressão. O compromisso deve especificar que a funcionalidade tem de ser devidamente protegida contra utilização abusiva (ou seja, a tática de «sinalização em massa» de modo a silenciar outras opiniões) e estar disponível em todas as línguas dos Estados-Membros da UE nas quais os seus serviços são prestados. As medidas tomadas pelos signatários relativamente a conteúdos sinalizados devem respeitar a liberdade de expressão e não devem ser desproporcionadas. As medidas neste domínio poderão incluir a aplicação de um procedimento transparente de verificação de factos ao conteúdo sinalizado, juntamente com ações posteriores de acompanhamento, como a rotulagem do conteúdo, quando pertinente. Os signatários devem comprometer-se a facultar aos utilizadores informações sobre o seguimento dado à denúncia, nomeadamente se o conteúdo foi examinado e, em caso afirmativo, quais os resultados da avaliação e as medidas tomadas em relação ao mesmo. Os utilizadores cujos conteúdos ou contas tenham sido alvo dessas medidas devem igualmente ser informados, a fim de compreenderem os motivos subjacentes e de terem acesso a um mecanismo adequado e transparente de recurso e obtenção de reparação.

7.7 Disponibilidade de indicadores que permitam uma navegação informada em linha

O código reforçado não tem como objetivo avaliar a veracidade do conteúdo editorial. Todavia, dada a quantidade de informações disponíveis em linha, os utilizadores têm dificuldade em determinar que fontes de informação podem consultar e são fiáveis. Centrados na integridade das fontes e desenvolvidos por terceiros independentes em colaboração com os meios de informação, incluindo associações de jornalistas, organizações de defesa da liberdade dos meios de comunicação social e verificadores de factos, os indicadores de fiabilidade podem ajudar os utilizadores a fazerem escolhas informadas⁶².

Os signatários poderão facilitar o acesso a esses indicadores, oferecendo aos utilizadores a possibilidade de os utilizarem nos seus serviços. Nesse caso, o código reforçado deve garantir que os signatários asseguram a transparência desses indicadores de terceiros, incluindo no que se refere à sua metodologia.

A aplicação desses indicadores de fiabilidade deve ser plenamente consonante com os princípios da liberdade e do pluralismo dos meios de comunicação social. Para tal, a utilização dos instrumentos deve ser deixada ao critério dos utilizadores⁶³.

⁶² São exemplo de tais indicadores o Índice Global de Desinformação (GDI), a Journalism Trust Initiative (JTI), o Trust Project ou ainda o serviço NewsGuard.

⁶³ Devem ser disponibilizados aos utilizadores instrumentos que permitam avaliar a fiabilidade das fontes de informação, como as chamadas marcas de confiança, para que possam consultá-los se assim o desejarem. Poderá também ser dada aos utilizadores a possibilidade de integrar sinais relacionados com a fiabilidade das fontes mediáticas nos sistemas automatizados que selecionam e classificam os conteúdos apresentados nos *feeds* do utilizador.

7.8 Medidas para travar a desinformação nas aplicações de mensagens

Além das recentes iniciativas desenvolvidas em cooperação com verificadores de factos⁶⁴, os signatários que disponibilizem aplicações de mensagens privadas devem testar e implementar funcionalidades técnicas que ajudem os utilizadores a identificar a desinformação divulgada através desses serviços. Essas soluções devem ser compatíveis com a natureza dos serviços e, em especial, com o direito às comunicações privadas, sem qualquer enfraquecimento da encriptação. As funcionalidades podem, por exemplo, ajudar os utilizadores a verificar se um determinado conteúdo que receberam foi sinalizado como falso na sequência de uma verificação de factos. Este objetivo poderá ser alcançado, por exemplo, mediante soluções que tornem os rótulos de verificação de factos visíveis quando os conteúdos das redes sociais são divulgados através de uma aplicação de mensagens. Os signatários poderão igualmente estudar soluções que permitam aos utilizadores confrontar os conteúdos que receberam numa aplicação de mensagens com um repositório de verificação de factos.

8 CAPACITAÇÃO DA COMUNIDADE DE INVESTIGAÇÃO E DE VERIFICAÇÃO DE FACTOS

Tendo em conta que a sua contribuição é fundamental para uma estratégia eficaz de combate à desinformação, o código reforçado deve prever um quadro que permita à comunidade de investigação e de verificação de factos ter um acesso estável aos dados da plataforma, bem como um apoio adequado às suas atividades.

8.1 Acesso aos dados dos signatários para efeitos de investigação em matéria de desinformação

Ao proporcionarem análises baseadas em dados, os investigadores são essenciais para uma boa compreensão da evolução dos riscos associados à desinformação⁶⁵ e podem contribuir para o desenvolvimento de mecanismos de atenuação de riscos. Este trabalho depende, de forma crítica, do acesso aos dados da plataforma. A proposta de RSD prevê um mecanismo regulador para que os investigadores habilitados tenham acesso aos dados para efeitos de investigação sobre os riscos decorrentes dos serviços das plataformas⁶⁶. O código reforçado deve criar um quadro que, no período que precede a adoção do RSD, já conceda aos investigadores o acesso necessário aos dados das plataformas e que, a longo prazo, também facilite o desenvolvimento de um quadro específico de acesso aos dados adaptado à realização de investigação sobre os fenómenos de desinformação.

8.1.1 Quadro geral de acesso aos dados

Os signatários pertinentes, em especial as plataformas, devem comprometer-se a cocriar, para o código reforçado, um quadro sólido de acesso aos dados para fins de investigação. As condições de acesso devem ser transparentes, abertas e não discriminatórias, proporcionadas e justificadas. No que diz respeito aos dados pessoais, as condições têm de estar em conformidade com o RGPD. Em geral, as condições de acesso a quaisquer

⁶⁴ As organizações de verificação de factos, apoiadas por alguns fornecedores de aplicações de mensagens, dão aos utilizadores das aplicações a possibilidade de verificarem os factos de mensagens que receberam através desses canais privados: https://faq.whatsapp.com/general/ifcn-fact-checking-organizations-on-whatsapp/?lang=pt_pt.

⁶⁵ Tal é igualmente fundamental para informar os signatários, a Comissão, as autoridades nacionais competentes e o público.

⁶⁶ Nomeadamente, o artigo 31.º.

dados devem respeitar o direito às comunicações privadas e proteger adequadamente os direitos e interesses legítimos de todas as partes em causa.

Os signatários devem desenvolver o quadro em cooperação com a comunidade de investigação, o EDMO e as autoridades nacionais competentes. Os compromissos devem incluir um calendário pormenorizado dos progressos esperados na conceção e na aplicação do quadro.

O quadro deve contemplar diferentes acessos a regimes de dados, com garantias adequadas para i) dados anonimizados e não pessoais e ii) dados que exijam controlo adicional, incluindo dados pessoais. O quadro deve prever a possibilidade de acesso em tempo real a determinados tipos de dados, de modo a permitir uma avaliação rápida dos riscos emergentes ou em evolução e a conceção de medidas de atenuação adequadas.

Enquanto o quadro se encontra em fase de desenvolvimento, os signatários devem testar soluções provisórias. Por exemplo, a utilização de «ambientes de testagem» poderá facultar a um número limitado de investigadores acesso a dados pertinentes da plataforma para fins de investigação sobre temas específicos, de modo a apoiar a conceção do quadro e testar soluções operacionais para um acesso mais amplo aos dados em todas as plataformas.

8.1.2 Acesso a dados anonimizados e não pessoais

O código reforçado deve incluir o compromisso de conceder, sempre que possível, acesso contínuo, em tempo real, estável e harmonizado a dados anonimizados, agregados ou não pessoais para fins de investigação, através de IPA ou de outras soluções técnicas abertas e acessíveis que permitam a plena exploração dos conjuntos de dados.

As soluções de acesso aos dados devem facilitar a pesquisa e a análise dos dados. Os signatários pertinentes devem garantir que as funcionalidades dos sistemas de acesso satisfazem as necessidades dos investigadores e são interoperáveis. Os compromissos devem assegurar procedimentos para a comunicação de anomalias nos sistemas de acesso e para a reposição do acesso e a reparação de funcionalidades defeituosas num prazo razoável.

8.1.3 Acesso a dados que exijam controlo adicional, incluindo dados pessoais

Os dados que possam expor informações pessoais, incluindo informações sensíveis⁶⁷, requerem segurança e garantias adicionais. As informações confidenciais, em especial segredos comerciais ou dados associados à segurança dos serviços das plataformas, carecem igualmente de uma proteção adequada. Simultaneamente, o quadro de acesso aos dados deve, no mínimo, permitir que os investigadores académicos acedam aos conjuntos de dados necessários para compreender as fontes, os vetores, os métodos e os padrões de propagação que caracterizam o fenómeno da desinformação.

Para tal, o código deve estabelecer um procedimento transparente que envolva todas as partes interessadas, em especial as plataformas e a comunidade de investigação, de modo a definir as condições aplicáveis ao acesso a estes conjuntos de dados. Em princípio, as condições devem ser normalizadas e uniformes em todas as plataformas. O procedimento deve regular, nomeadamente, i) as normas mínimas e as qualificações dos investigadores

⁶⁷ Na aceção do artigo 9.º do RGPD.

a quem será concedido acesso; ii) as categorias mínimas de dados que serão disponibilizadas; iii) as medidas de segurança técnicas e organizativas a cumprir no tratamento dos dados, incluindo a limitação da finalidade e a minimização dos dados; e iv) relativamente aos dados pseudonimizados, quaisquer medidas necessárias para impedir a reatribuição⁶⁸.

8.1.4 Funções do EDMO

Tendo em conta a sua independência e as suas funções de coordenação, o EDMO poderá prestar apoio no domínio do acesso aos dados, incluindo orientações relativas, nomeadamente, às categorias de dados a disponibilizar, às finalidades para as quais os dados podem ser tratados e às medidas de segurança adequadas para o tratamento de dados pessoais e para impedir a reatribuição de dados anonimizados.

Estão a ser desenvolvidos trabalhos, facilitados pelo EDMO, a fim de explorar as possibilidades de um código de conduta nos termos do artigo 40.º do RGPD, que vise assegurar a aplicação adequada dos requisitos em matéria de privacidade e de proteção de dados à partilha, pelas plataformas, de dados pessoais com os investigadores. O RGPD prevê condições gerais para o tratamento de dados pessoais também sob a forma de partilha, pelas plataformas, de dados pessoais com os investigadores. O referido código reduziria as inseguranças jurídicas e os riscos para as plataformas que disponibilizam acesso aos dados e asseguraria um ambiente seguro e harmonizado para o tratamento de dados pessoais para fins de investigação⁶⁹. O código reforçado deve exigir que os signatários se comprometam a facilitar, conforme necessário, o desenvolvimento do código de conduta nos termos do artigo 40.º do RGPD.

8.1.5 Acesso de outras partes interessadas aos dados

Outras partes interessadas, tais como organizações da sociedade civil, centros de investigação não académicos e jornalistas de investigação, desempenham igualmente funções importantes na deteção e na análise de campanhas de desinformação, na definição de respostas políticas, bem como na promoção da sensibilização do público e da resiliência social. Os signatários do código devem permitir, em especial nos Estados-Membros onde não exista uma capacidade académica adequada, um nível de acesso suficiente para essas partes interessadas, coerente com os requisitos de privacidade e sujeito a um controlo reforçado contra a utilização abusiva de dados pessoais e a reatribuição de dados pseudonimizados.

8.2 Quadro de cooperação entre os signatários e os investigadores

A fim de promover e capacitar uma comunidade multidisciplinar mais ampla de investigadores independentes, o código deve estabelecer um quadro para uma cooperação transparente, aberta e não discriminatória entre os signatários e a comunidade de investigação da UE no que respeita aos recursos e ao apoio disponibilizados aos investigadores. Este quadro deve permitir à comunidade de investigação gerir de forma independente os fundos disponibilizados pelos signatários para fins de investigação em

⁶⁸ Conforme exigido pelo RGPD, a divulgação de dados pessoais deve basear-se num fundamento jurídico claro, com garantias adequadas, incluindo o regime do artigo 9.º para as categorias especiais de dados.

⁶⁹ O debate das partes interessadas demonstrou o apoio dos signatários do código e da comunidade de investigação a esta iniciativa: <https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation>.

matéria de desinformação, definindo prioridades científicas e procedimentos transparentes de atribuição com base no mérito científico. Neste contexto, o EDMO poderá ajudar a atribuir os recursos.

8.3 Colaboração com os verificadores de factos

Os verificadores de factos são intervenientes importantes na resposta ao fenómeno da desinformação⁷⁰. Avaliam e verificam os conteúdos com base em factos, dados e informações contextuais e sensibilizam os utilizadores para a desinformação em linha. O código reforçado deve prever um apoio acrescido ao seu trabalho e aumentar a abrangência das atividades de verificação de factos nos Estados-Membros e nas línguas da UE.

8.3.1 Formas de cooperação

Tendo em conta as lacunas significativas e a aplicação desigual das atividades de verificação de factos nos serviços e nos Estados-Membros⁷¹, a plataformas signatárias devem comprometer-se a tomar medidas concretas, com metas e calendários claros, para ampliar a sua cooperação com os verificadores de factos, de modo a assegurar a aplicação coerente da verificação de factos nos seus serviços. Os esforços devem centrar-se, em especial, nos Estados-Membros e nas línguas em que a verificação de factos ainda não é disponibilizada⁷².

Tal poderá ser alcançado através de acordos multilaterais entre plataformas e organizações independentes de verificação de factos que cumpram elevadas normas éticas e profissionais. Os acordos devem basear-se em condições transparentes, abertas e não discriminatórias e assegurar a independência dos verificadores de factos. Devem ainda prever uma remuneração justa dos verificadores de factos por trabalhos utilizados pelas plataformas, promover a cooperação transfronteiriça entre verificadores de factos e facilitar o fluxo de verificações de factos entre os serviços dos signatários.

Tendo em conta a sua função na promoção de atividades conjuntas de verificação de factos, o EDMO encontra-se numa posição privilegiada para prestar apoio às plataformas e aos verificadores de factos no desenvolvimento de um quadro de colaboração, incluindo no que respeita à criação de uma interface comum para verificadores de factos, ao intercâmbio de informações entre verificadores de factos e à promoção da cooperação transfronteiriça⁷³.

⁷⁰ As organizações de verificação de factos publicam regularmente relatórios apartidários sobre a exatidão das declarações de figuras públicas e instituições de renome e de outras alegações de interesse para a sociedade amplamente divulgadas. São independentes e seguem regras éticas e de transparência rigorosas, tal como a definida pela Rede Internacional de Verificação de Factos (IFCN) (<https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles>).

⁷¹ <https://www.disinfo.eu/publications/bulgaria%3A-the-wild-wild-east-of-vaccine-disinformation/>.

⁷² Mapa das atividades de verificação de factos na UE, do EDMO: <https://edmo.eu/fact-checking-activities/>.

⁷³ A fim de reforçar o apoio ao trabalho dos verificadores de factos europeus, à sua cooperação e ao desenvolvimento de normas profissionais comumente acordadas, o projeto-piloto «Integrity of social media» [Integridade das redes sociais] apoiará a elaboração de um código de integridade profissional para os verificadores de factos europeus, em cooperação com o EDMO. Ver: programa de trabalho anual, adotado nos termos da Decisão C(2020)2259 da Comissão.

8.3.2 Utilização e integração da verificação de factos nos serviços dos signatários

O código reforçado deve incluir compromissos que exijam a utilização e a integração mais coerentes do trabalho dos verificadores de factos nos serviços das plataformas, incluindo nos sistemas de publicidade programática e nos conteúdos de vídeo. As plataformas devem comprometer-se a utilizar mecanismos que permitam a incorporação imediata e coerente de verificações de factos nos seus serviços mediante notificação dos verificadores de factos, incluindo uma rotulagem rápida e eficaz. Os signatários devem facilitar a criação de um repositório comum de artigos de verificação de factos (verificações de factos) elaborados por verificadores de factos e explorar soluções tecnológicas para facilitar a sua utilização eficaz em todas as plataformas e línguas, de modo a impedir que a desinformação denunciada pelos verificadores de factos volte a surgir⁷⁴.

8.3.3 Acesso dos verificadores de factos a informações pertinentes

A fim de maximizar a qualidade e o impacto da verificação de factos, o código reforçado deve assegurar que as plataformas signatárias se comprometem a disponibilizar aos verificadores de factos um acesso automatizado às informações relativas às medidas tomadas no que respeita aos conteúdos cujos factos foram verificados e às verificações dos factos. As informações devem quantificar i) as interações dos utilizadores ao longo do tempo (por exemplo, o número de visualizações, de menções «gosto», de partilhas, de comentários anteriores e posteriores à verificação de factos)⁷⁵ com os conteúdos cujos factos foram verificados, e ii) o alcance da verificação de factos ao longo do tempo nos serviços em linha nos quais foram publicados. As plataformas e os verificadores de factos devem chegar a acordo sobre uma interface comum para a verificação de factos, de modo a assegurar a coerência na forma como as plataformas utilizam, credibilizam e comentam o trabalho dos verificadores de factos. Além disso, o código deve prever um intercâmbio regular de informações entre os signatários pertinentes do código e a comunidade de verificação de factos, com o objetivo de continuar a reforçar a cooperação.

9 ACOMPANHAMENTO DO CÓDIGO

O código reforçado deve ser complementado com um sistema de acompanhamento sólido, com base na experiência da Comissão até à data no que diz respeito ao acompanhamento do código, incluindo o programa relativo à COVID-19. O sistema de acompanhamento melhorado deve prever a avaliação periódica da aplicação dos compromissos do código pelos signatários, incentivar melhorias nas suas políticas e medidas e permitir a avaliação da eficácia do código enquanto instrumento para combater a desinformação. O sistema de acompanhamento melhorado deve reforçar a responsabilização das plataformas em linha no período que precede a adoção do RSD e proporcionar um quadro para, nomeadamente, um diálogo estruturado com plataformas de muito grande dimensão a respeito do desenvolvimento e da implementação de medidas de avaliação e atenuação de riscos, na pendência das obrigações legais que lhes estão destinadas na proposta de RSD.

⁷⁴ No que diz respeito à criação de um repositório de verificações de factos, os signatários poderão procurar estabelecer sinergias com o EDMO.

⁷⁵ Tal deve incluir igualmente dados demográficos anonimizados e a localização de quem partilha/recebe conteúdos cujos factos foram verificados.

Tendo em conta estes objetivos, os atuais compromissos do código relativos ao acompanhamento devem ser reforçados e ampliados, a fim de criar um quadro sólido que inclua os elementos fundamentais a seguir enunciados. O código reforçado deve assegurar, em especial, que os signatários facultam as informações e os dados necessários para o acompanhamento em formatos normalizados, discriminados por Estado-Membro e em tempo útil.

9.1 Indicadores-chave de desempenho

O acompanhamento do código deve apoiar-se em ICD capazes de medir a aplicação e a eficácia dos compromissos do código e o respetivo impacto no fenómeno da desinformação. Para tal, são pertinentes duas categorias de ICD: i) indicadores do nível de serviço, que medem os resultados e o impacto das políticas implementadas pelos signatários para cumprir os compromissos assumidos nos termos do código, e ii) indicadores estruturais, que medem o impacto global do código na desinformação existente na UE.

9.1.1 Indicadores do nível de serviço

Nos termos do código revisto, os signatários devem comprometer-se a definir indicadores concretos do nível de serviço. Os indicadores do nível de serviço devem medir eficazmente a aplicação dos compromissos do código e o impacto das políticas dos signatários. Os indicadores devem ser suficientemente flexíveis para ter em conta a natureza distinta dos serviços dos signatários, permitindo, simultaneamente, relatórios e comparações coerentes entre os serviços.

O código reforçado deve exigir que os signatários identifiquem, comuniquem e se comprometam com um conjunto mínimo de indicadores qualitativos e quantitativos que visem avaliar, nomeadamente:

- o impacto das funcionalidades e dos instrumentos implementados para aumentar a sensibilização e a capacitação dos utilizadores, incluindo as interações dos utilizadores com os mesmos⁷⁶,
- o impacto dos instrumentos e das funcionalidades que apresentam ou conferem mais visibilidade a informações fidedignas de interesse público, incluindo as interações dos utilizadores com os mesmos⁷⁷,
- o número de verificações de factos, a percentagem de conteúdos cujos factos foram verificados em comparação com a percentagem de conteúdos sinalizados pelos utilizadores e o financiamento concedido a atividades de verificação de factos,
- o impacto das atividades de verificação de factos e das interações dos utilizadores com as informações cujos factos foram verificados e sinalizados como falsos ou enganosos⁷⁸,

⁷⁶ O impacto poderá ser medido através de indicadores que quantifiquem o nível de interação (por exemplo, visualizações, taxas de cliques, partilhas, etc.) dos utilizadores com esses instrumentos e que qualifiquem a sua perceção da utilidade dos mesmos. Além disso, os indicadores devem incluir dados sobre a utilização de instrumentos para sinalizar e denunciar conteúdos considerados falsos.

⁷⁷ O impacto poderá ser medido através de indicadores que quantifiquem o nível de interação (por exemplo, visualizações, impressões, taxas de cliques, partilhas, etc.) dos utilizadores com esses instrumentos e que qualifiquem a sua perceção da utilidade dos mesmos.

- o número de recursos relativos a medidas adotadas pelas plataformas em relação a conteúdos, na sequência da sinalização da desinformação, e informações sobre o respetivo resultado,
- o número de páginas, contas, perfis e grupos que partilham desinformação sujeitos a medidas que visam reduzir a respetiva visibilidade⁷⁹ e a quantidade de conteúdo partilhado,
- o impacto de comportamentos manipuladores inadmissíveis identificados, incluindo situações de contas ou de conteúdos removidos ou despromovidos⁸⁰,
- o número de parcerias entre os signatários do código do setor da publicidade e entidades terceiras que avaliam a qualidade das fontes de informação,
- o impacto das medidas utilizadas para efeitos de controlo da colocação de anúncios⁸¹,
- a quantidade e a granularidade dos dados disponibilizados para fins de investigação e o número de organizações europeias de investigação que têm acesso aos dados das plataformas,
- a quantidade de recursos disponibilizados pelos signatários para a investigação em matéria de desinformação e o número de organizações europeias de investigação que têm acesso aos mesmos,
- informações relativas à mão de obra humana envolvida no cumprimento dos compromissos do código⁸².

9.1.2 Indicadores estruturais

Os signatários do código devem igualmente comprometer-se a contribuir para o desenvolvimento de indicadores estruturais capazes de medir eficazmente o impacto global do código no fenómeno da desinformação. Como adiante descrito de forma mais pormenorizada, os signatários devem criar um grupo de trabalho permanente cujas funções incluirão o desenvolvimento, a testagem e o ajustamento dos indicadores estruturais.

Os indicadores estruturais poderão, por exemplo, basear-se em amostras representativas dos utilizadores de vários Estados-Membros, com o objetivo de aferir a prevalência de agentes de desinformação persistentes⁸³ no consumo de meios de comunicação em linha

⁷⁸ O impacto poderá ser medido através de indicadores que quantifiquem o nível de interação (por exemplo, visualizações, taxas de cliques, partilhas) com conteúdos antes e depois de serem rotulados ou despromovidos por terem sido sinalizados como falsos. Outros indicadores poderão igualmente facultar informações sobre a forma como as interações dos utilizadores ocorrem.

⁷⁹ Incluindo medidas como a desclassificação de conteúdos, bem como o encerramento de perfis e de grupos.

⁸⁰ O impacto poderá ser medido através de indicadores que quantifiquem o nível de interação (por exemplo, visualizações, taxas de cliques, partilhas, etc.) com os conteúdos, contas e situações antes de serem removidos e antes e depois de serem despromovidos.

⁸¹ O impacto poderá ser medido através de indicadores que quantifiquem o número de anúncios colocados e apresentados em sítios Web identificados como agentes persistentes de desinformação, e o número de anúncios que incluíam desinformação que foram removidos.

⁸² Inclui o número de trabalhadores contratados para executar atividades que visam combater a desinformação e as línguas abrangidas pelas suas atividades.

⁸³ A identificação de agentes desinformadores em linha deve basear-se numa metodologia clara e acordada, definida por um conjunto mais vasto de partes interessadas, incluindo investigadores académicos, verificadores de factos, ONG e organizações da sociedade civil.

dos cidadãos europeus⁸⁴. Tais indicadores poderão medir o envolvimento do público com fontes de informação, bem como inquéritos regulares e normalizados para medir a exposição dos cidadãos à desinformação.

Até que seja desenvolvido um conjunto mais estável de indicadores estruturais, os signatários e as partes interessadas devem chegar a acordo quanto a um conjunto mínimo viável de indicadores estruturais que possam ser rapidamente implementados e testados, envidando esforços no sentido de desenvolver um conjunto estável de indicadores estruturais eficazes.

9.2 Quadro de acompanhamento

O quadro de acompanhamento deve permitir a avaliação periódica da aplicação dos compromissos do código pelos signatários, incluindo das alterações e dos desenvolvimentos das políticas e das medidas pertinentes. Para tal, os signatários devem informar regularmente a Comissão sobre a aplicação dos seus compromissos, incluindo os ICD pertinentes.

Após a experiência positiva dos programas de monitorização durante as eleições de 2019 da UE⁸⁵ e a pandemia de COVID-19, a Comissão contará com o apoio do Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual (ERGA) no acompanhamento da aplicação do código a nível dos Estados-Membros. O EDMO e os respetivos centros devem apoiar igualmente a Comissão na análise das informações e dos dados comunicados pelos signatários e na avaliação do impacto do código a nível nacional e da UE.

Tendo em conta o parecer dos peritos e o apoio do ERGA e do EDMO, a Comissão avaliará periodicamente os progressos alcançados na aplicação do código, bem como o impacto do código no fenómeno da desinformação, e publicará as suas conclusões. A Comissão pode igualmente facultar orientações adicionais relativas à forma como os signatários devem dar resposta às insuficiências e às lacunas subsistentes no código.

9.2.1 Relatórios periódicos

As obrigações de apresentação de relatórios ao abrigo do código reforçado devem ter em conta a dimensão dos signatários e o tipo de serviços que prestam. Os prestadores de serviços em linha que são amplamente utilizados a nível da UE e que apresentam perfis de risco mais elevado no que diz respeito à disseminação da desinformação devem apresentar relatórios semestrais sobre a aplicação dos compromissos que subscreveram e devem facultar os indicadores correspondentes do nível de serviço. Devem igualmente, numa base anual, avaliar os riscos associados ao fenómeno da desinformação. Os outros signatários do código devem apresentar um relatório anual e facultar os dados correspondentes às suas atividades. Os signatários que disponibilizam ferramentas, instrumentos ou soluções para combater a desinformação, ou que apoiam o código mediante a disponibilização de conhecimentos especializados, devem igualmente, numa base anual, comunicar as suas atividades e conclusões que forem pertinentes para a aplicação e para a eficácia do código. Os relatórios devem ser elaborados de acordo com

⁸⁴ O mecanismo de medição para indicadores estruturais poderá inspirar-se nos métodos utilizados pelo setor audiovisual para determinar as audiências.

⁸⁵ <https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf>.

um calendário definido que estabeleça os períodos de cobertura e os prazos de envio. Os dados utilizados para medir os ICD devem incluir discriminações por Estado-Membro.

Os relatórios devem basear-se num modelo harmonizado que permita, na medida do possível, comparações entre plataformas. Além disso, os signatários devem chegar a acordo quanto a um conjunto de formatos normalizados e passíveis de auditoria para a apresentação dos dados relacionados com os ICD. Estes formatos devem ser desenvolvidos em conjunto com as partes interessadas do grupo de trabalho permanente e devem cumprir as normas e utilizar os métodos da comunidade de investigação e de verificação de factos. Eventualmente, estes formatos devem permitir a atualização contínua de um painel público, disponibilizado pelo centro de transparência, tal como descrito a seguir.

9.2.2 Centro de transparência

A fim de reforçar a transparência e a responsabilização no que respeita à aplicação do código, os signatários devem comprometer-se a criar e a manter um centro de transparência acessível ao público. Os signatários devem indicar, no centro de transparência, as políticas específicas que adotaram para aplicar cada compromisso do código que subscreveram e facultar informações básicas sobre a forma como estas políticas são aplicadas, incluindo a cobertura geográfica e linguística. O centro de transparência deve incluir igualmente um painel público que apresente os ICD pertinentes. Deve ser concebido, em especial, de modo a permitir comparações interserviços dos progressos dos signatários na aplicação dos compromissos do código e na consecução de impactos quantificáveis no combate à desinformação. Os signatários devem comprometer-se a atualizar regularmente o centro de transparência e a divulgar quaisquer alterações das políticas pertinentes o mais tardar 30 dias após ser anunciada ou introduzida uma alteração.

9.2.3 Grupo de trabalho permanente

O código reforçado deve criar um grupo de trabalho permanente que vise o desenvolvimento e a adaptação do código em função da evolução tecnológica, societal, legislativa e do mercado. O grupo de trabalho deve incluir os signatários do código e representantes do EDMO e do ERGA e poderá convidar peritos de domínios pertinentes, a fim de prestarem apoio ao seu trabalho. O grupo de trabalho deve ser presidido pela Comissão e incluir representantes do Serviço Europeu para a Ação Externa. Em consonância com o objetivo geral de contribuir para a revisão e a adaptação do código, as atividades do grupo de trabalho devem incluir, nomeadamente:

- estabelecer uma metodologia de avaliação de riscos e um sistema de resposta rápida a utilizar em situações especiais, como eleições ou crises,
- rever a qualidade e a eficácia do modelo de relatório harmonizado, bem como os formatos e os métodos de divulgação de dados para fins de acompanhamento,
- otimizar a qualidade e a exatidão dos dados a facultar para a medição dos indicadores,
- contribuir para a avaliação da qualidade e da eficácia dos indicadores do nível de serviço e para a respetiva adaptação pertinente,
- desenvolver, testar e ajustar os indicadores estruturais e conceber mecanismos que permitam medi-los a nível dos Estados-Membros;
- fornecer contributos de peritos e dados atualizados pertinentes para os compromissos do código, nomeadamente sobre novas formas de comportamento inautêntico.

10 CONCLUSÃO E PRÓXIMAS ETAPAS

As presentes orientações estabelecem os elementos fundamentais que, na opinião da Comissão, são necessários para transformar o código num instrumento mais forte, a fim de combater a desinformação e de criar um ambiente em linha mais seguro e mais transparente.

A Comissão insta os signatários do código a reunirem-se e a reforçarem o código, em consonância com as presentes orientações. A Comissão convida os signatários a apresentarem um primeiro projeto de código revisto no outono, a fim de permitir um debate adequado. Convida igualmente os potenciais novos signatários a aderirem ao código e a participarem na sua revisão, incluindo plataformas estabelecidas e emergentes, intervenientes empresariais e outros participantes no setor da publicidade em linha, bem como outras partes interessadas que possam contribuir com recursos ou conhecimentos especializados para o funcionamento eficaz do código.

Uma vez que a desinformação é um fenómeno sem fronteiras, e a fim de reforçar o impacto real do código de conduta, seria útil desenvolver ações na vizinhança europeia, nomeadamente em termos de trabalho com a sociedade civil, cooperação com profissionais dos meios de comunicação social e iniciativas de literacia mediática.