COMMISSION
EUROPÉENNE

Bruxelles, le 26.5.2021
COM(2021) 262 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Orientations de la Commission européenne visant à renforcer le code européen de bonnes pratiques contre la désinformation

1 INTRODUCTION

La crise de la COVID-19 illustre de manière saisissante les menaces et les dangers que la désinformation représente pour nos sociétés. L'«infodémie», c'est-à-dire la diffusion rapide d'informations fausses, inexactes ou trompeuses sur la pandémie, fait peser des risques considérables sur la santé des personnes, les systèmes de santé publique, la gestion efficace des crises, l'économie et la cohésion sociale. La pandémie a également renforcé le rôle que jouent les technologies numériques dans nos vies. Elles occupent désormais une place de plus en plus importante dans la manière dont nous travaillons, nous apprenons, nous socialisons, nous subvenons à nos besoins matériels et nous participons au discours civique. Elle a accru les enjeux, car il était nécessaire de garantir la sécurité de l'écosystème en ligne et elle a montré que, malgré les efforts considérables déployés jusqu'à présent, il est urgent d'intensifier nos efforts dans le cadre de la lutte contre la désinformation[1].

Dès le départ[2], l'approche de l'Union en matière de lutte contre la désinformation s'est fondée sur la protection de la liberté d'expression et des autres droits et libertés garantis par la Charte des droits fondamentaux de l'UE. Dans le respect de ces droits et libertés, plutôt que de criminaliser ou d'interdire la désinformation en tant que telle, la stratégie de l'Union vise à rendre l'environnement en ligne et ses acteurs plus transparents et plus responsables, en renforçant la transparence des pratiques de modération des contenus, en responsabilisant les citoyens et en favorisant un débat démocratique ouvert[3]. À cette fin, l'Union européenne a cherché à mobiliser toutes les parties prenantes concernées, notamment les pouvoirs publics, les entreprises, les médias, la sphère universitaire et la société civile.

Le code de bonnes pratiques contre la désinformation[4] est un texte d'autoréglementation qui constitue une pièce maîtresse des efforts de l'Union en la matière. Il est en vigueur depuis octobre 2018 et ses signataires comprennent désormais les principales plateformes en ligne actives dans l'Union ainsi que, entre autres, les grandes associations professionnelles représentant le secteur européen de la publicité. La Commission considère que ce code est une réalisation majeure, la première du genre. Il constitue un outil novateur permettant de garantir la transparence et l'obligation de rendre compte des plateformes en ligne et offre un cadre structuré pour le suivi et l'amélioration des politiques des plateformes en matière de désinformation.

Cependant, l'évaluation du code de bonnes pratiques par la Commission en 2020[5] a révélé des lacunes importantes, notamment une application incohérente et incomplète du code sur les plateformes et dans les États membres, des limites intrinsèques au caractère autorégulateur du code, ainsi que des lacunes dans la couverture des engagements du code. L'évaluation a également mis en évidence l'absence de mécanisme de suivi

[1]Communication conjointe, Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux [JOIN(2020) 8 final].
[2]Dans le Plan d'action contre la désinformation (JOIN (2018) 36 final), la Commission européenne et la haute représentante ont défini une stratégie globale visant à lutter contre la désinformation au sein de l'Union.
[3]Si les conditions générales des plateformes en ligne peuvent aussi couvrir les contenus préjudiciables mais non illicites, lorsque la désinformation constitue un contenu illicite (par exemple, les discours haineux ou les contenus à caractère terroriste), les recours législatifs pertinents s'appliquent.
[4]https://ec.europa.eu/digital-single-market/en/code-practice-disinformation
[5]SWD (2020) 180 final.

approprié, notamment d'indicateurs clés de performance (ICP), le manque d'engagement concernant l'accès aux données des plateformes pour la recherche sur la désinformation et la participation limitée des parties prenantes, en particulier dans le secteur de la publicité. Par conséquent, la Commission a annoncé dans le plan d'action pour la démocratie européenne[6] qu'elle publiera une orientation sur le renforcement du code, dans le cadre d'actions globales visant à lutter contre la désinformation dans l'environnement en ligne, et qu'elle présentera une législation spécifique concernant la transparence de la publicité à caractère politique.

Afin d'intensifier la lutte contre la désinformation, la législation sur les services numériques[7] proposée par la Commission définit un cadre de corégulation par l'intermédiaire de codes de conduite pour faire face aux risques systémiques liés à la désinformation. En outre, elle instaure des mesures de transparence de grande ampleur concernant la modération de contenus et la publicité, et propose des obligations juridiques contraignantes et exécutoires pour les très grandes plateformes en ligne [8] afin d'évaluer les risques systémiques qui menacent les droits fondamentaux ou ceux que présente la manipulation intentionnelle de leur service, et de faire face à ces risques.

Les orientations se fondent sur l'expérience acquise jusqu'à présent par la Commission concernant le suivi et l'évaluation du code[9] et sur le rapport de la Commission sur les élections de 2019[10]. Elles contribuent également à la réponse de la Commission aux conclusions du Conseil européen de décembre 2020[11]. Afin de recueillir des contributions pour ces orientations, la Commission a organisé des discussions multipartites[12] ainsi qu'un atelier destiné aux États membres.

Les présentes orientations exposent le point de vue de la Commission sur la manière dont les plateformes et les autres parties prenantes concernées devraient renforcer leurs mesures visant à combler les lacunes et les insuffisances du code et créer un environnement en ligne plus transparent, plus sûr et plus fiable. Un domaine, en particulier, dans lequel le code n'a pas permis de réaliser des progrès suffisants est celui de la démonétisation de la désinformation, c'est-à-dire les cas dans lesquels les publicités en ligne continuent d'encourager la diffusion d'éléments de désinformation[13]. Les

---

[6]COM (2020) 790 final.

[7]Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE [COM(2020) 825 final]. Dans le présent document, les références à la législation sur les services numériques doivent être comprises comme le texte tel que proposé par la Commission.

[8]À l'article 25, la proposition relative à la législation sur les services numériques définit les très grandes plateformes comme des plateformes en ligne fournissant leurs services à un nombre mensuel moyen de bénéficiaires actifs du service au sein de l'Union correspondant à 10 % de la population de l'Union.

[9]Évaluation de la Commission de septembre 2020 [SWD (2020) 180 final]

[10]Rapport sur les élections au Parlement européen de 2019 [SWD (2020) 113 final] https://ec.europa.eu/info/files/com_2020_252_en.pdf_en

[11]https://data.consilium.europa.eu/doc/document/ST-22-2020-INIT/fr/pdf

[12]Un résumé des discussions avec les parties prenantes est disponible à l'adresse suivante: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation

[13]Il est également prouvé que les recettes des publicités en ligne contribuent toujours de manière significative à la monétisation des sites web de désinformation, notamment les publicités de grandes marques placées involontairement à proximité de contenus de désinformation (par exemple, le rapport de l'indice mondial de la désinformation https://disinformationindex.org/2020/03/why-is-ad-tech-giving-

plateformes en ligne et tous les autres acteurs de l'écosystème de la publicité en ligne devraient donc prendre leurs responsabilités et coopérer pour démonétiser la désinformation. En outre, la révision du code devrait permettre de renforcer les engagements visant à limiter les comportements manipulateurs, à renforcer les outils de responsabilisation des utilisateurs, à accroître la transparence de la publicité à caractère politique et à donner plus de moyens à la communauté des vérificateurs de faits et des chercheurs. Les orientations détaillent aussi les fondements d'un cadre amélioré et solide permettant de suivre ce code renforcé, qui devrait également viser une participation plus large avec de nouveaux signataires, y compris d'autres plateformes en ligne actives dans l'Union ainsi que d'autres acteurs pertinents.

Le renforcement du code permet aux parties prenantes de concevoir à un stade précoce des mesures appropriées en vue de l'adoption de la proposition relative à la législation sur les services numériques. En particulier, les orientations visent aussi à faire évoluer le code de bonnes pratiques existant pour en faire un «code de conduite», comme le prévoit l'article 35. Les très grandes plateformes[14], notamment, bénéficieront de la participation au code renforcé en prévision des nouvelles obligations auxquelles elles seront soumises en vertu de la proposition relative à la législation sur les services numériques, notamment en ce qui concerne l'évaluation et l'atténuation des risques, la responsabilisation des utilisateurs et la transparence en matière de publicité. Les plateformes de plus petite taille et les autres parties prenantes auront également intérêt à souscrire aux engagements appropriés au titre du code renforcé afin de bénéficier de ses bonnes pratiques et de se prémunir contre les risques pour leur réputation liés à l'utilisation abusive de leurs systèmes en vue de propager des éléments de désinformation.

Sans préjudice de l'accord final des colégislateurs relatif à la législation sur les services numériques ou à l'initiative législative de la Commission concernant la transparence de la publicité à caractère politique, le code de bonnes pratiques renforcé peut servir d'outil permettant aux plateformes en ligne d'améliorer leurs politiques et d'atténuer les risques liés à la désinformation que leurs services présentent pour la démocratie.

Le renforcement du code ne constitue pas seulement une étape provisoire. Les présentes orientations prévoient que le code soit un instrument solide, stable et souple permettant de faire en sorte que les plateformes en ligne soient plus transparentes et plus responsables et davantage tenues de rendre des comptes.

2 SUIVI DE LA COVID-19 – RESULTATS ET ENSEIGNEMENTS TIRES

Outre les enseignements tirés de l'évaluation du code de bonnes pratiques, de nouvelles informations ont été recueillies dans le cadre du programme de suivi mis en place à la suite de la Communication conjointe intitulée: «Lutter contre la désinformation concernant la COVID-19»[15], au cours duquel les plateformes en ligne signataires du code

---

millions-to-eu-disinformation-sites/ et le rapport d'Avaaz https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/)

[14] Au sens de l'article 25 de la législation sur les services numériques telle que proposée par la Commission. Pour la définition, voir la note de bas de page nº 8.

[15] Communication conjointe, Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux [JOIN(2020) 8 final].

rendent compte chaque mois des mesures prises pour lutter contre la désinformation liée à la COVID-19 au sein de l'Union.

Le programme de suivi, qui recense les actions entreprises pour lutter contre la désinformation relative à la COVID-19 sur la base des engagements du code, soumet également le code à un «test de résistance».

Les rapports des plateformes indiquent que les engagements du code ont été mis en œuvre au moyen de mesures efficaces dans divers domaines, notamment une visibilité accrue, sur leurs services, des sources faisant autorité; la mise au point et le déploiement de nouveaux outils et services visant à faciliter l'accès à des informations fiables; des mesures visant à lutter contre les contenus présentant des informations fausses ou trompeuses susceptibles de causer des dommages physiques ou de nuire à l'efficacité des politiques de santé publique; l'interdiction expresse de la publicité qui exploite la crise ou propage des éléments de désinformation sur la COVID-19.

Dans l'ensemble, le programme a démontré que le code fournit un cadre agile et structuré qui peut être déployé et se traduire par des actions décisives des signataires en vue de lutter contre la désinformation dans les situations de crise et qui complète les obligations imposées par les cadres réglementaires applicables. Le code a également fourni une structure utile pour le suivi des mesures prises dans une situation extraordinaire, en procédant à un recentrage dynamique au fur et à mesure de l'évolution de la crise (par exemple, pour s'intéresser davantage à la désinformation entourant les vaccins contre la COVID-19).

Dans le même temps, le programme relatif à la COVID-19 a mis en lumière un certain nombre de lacunes présentées par le cadre de suivi existant du code de bonnes pratiques:

- *La qualité des rapports.* La cohérence, la qualité et le niveau de détail des rapports sont très variables. Du fait de l'absence de données présentant un niveau de détail suffisant, notamment à l'échelle des États membres, les informations fournies ne permettent souvent pas de savoir si les actions signalées ont été mises en œuvre dans tous les États membres ou dans toutes les langues de l'UE. En outre, l'absence de modèle de rapport commun et convenu demeure un obstacle pour un suivi plus efficace et des comparaisons entre les plateformes.
- *Les ICP.* Si la qualité et le niveau de détail des rapports se sont améliorés au fil du temps, les données communiquées ne sont pas toujours adéquates et suffisamment détaillées pour mesurer le degré de mise en œuvre des engagements ou l'effet des actions entreprises.
- *Une évaluation indépendante*. Le suivi de la COVID-19 a confirmé qu'il était nécessaire de procéder à une vérification indépendante des rapports des signataires, en particulier pour savoir si les politiques et les actions présentées dans les rapports ont été mises en œuvre au niveau des États membres et dans toutes les langues de l'UE et si les rapports abordent de manière adéquate les préoccupations en matière de désinformation au niveau national[16].
- *Une couverture insuffisante en matière de vérification des faits.* Au cours de l'«infodémie» concernant la COVID-19, les signataires ont renforcé les activités de

[16]Comme prévu dans la communication de juin 2020, le groupe des régulateurs européens pour les services de médias audiovisuels apporte son aide à la Commission en ce qui concerne le programme de suivi relatif à la COVID-19.

vérification des faits sur leurs services, qui deviennent également accessibles aux utilisateurs des applications de messagerie privée. Toutefois, les contenus que les vérificateurs de faits indépendants qualifient d'erronés ont tendance à ressurgir sur toutes les plateformes, faute d'une base centralisée répertoriant les vérifications de faits.

- *La monétisation continue de la désinformation par l'intermédiaire des placements de publicité.* Malgré les mesures visant à limiter la monétisation de la désinformation, des recherches pertinentes montrent qu'il subsiste des problèmes dans ce domaine[17].

3 QUESTIONS HORIZONTALES A ABORDER

3.1 Le renforcement des engagements en vue d'atteindre les objectifs du code

Les engagements du code de bonnes pratiques actuel ne sont pas suffisamment efficaces pour apporter une réponse globale au phénomène de la désinformation. Il est nécessaire de prendre des engagements plus forts et plus spécifiques dans tous les domaines du code afin de combler les lacunes et les insuffisances, notamment les risques nouveaux et émergents. Afin que le code reste un instrument vivant, les signataires devraient mettre en place un mécanisme permanent permettant de l'adapter régulièrement.

3.2 Un champ d'application élargi

L'«infodémie» liée à la pandémie de COVID-19 a démontré que la mésinformation[18] (informations fausses ou trompeuses diffusées sans intention malveillante) est également susceptible de causer un préjudice public important si elle devient virale. Si la cible principale reste la désinformation au sens strict[19], les signataires du code renforcé devraient s'engager à mettre en place des politiques appropriées et à prendre des mesures proportionnées afin d'atténuer les risques posés par la mésinformation, lorsqu'il existe une dimension de préjudice public important, et prévoir des garanties appropriées concernant la liberté d'expression. Les utilisateurs doivent avoir les moyens de comparer ces informations à des sources faisant autorité et être informés lorsque les informations qu'ils consultent sont manifestement fausses. En conséquence, en fonction de leur nature, tous les engagements du code ne s'appliquent pas à la mésinformation.

---

[17]Les recherches menées par l'indice mondial de la désinformation en janvier et février 2021 pour l'Allemagne, l'Espagne, la France et l'Italie soulignent que la majorité des entreprises de technologie publicitaire ne disposent pas de politiques spécifiques concernant les contenus de désinformation relatifs à la COVID-19 ou que ces politiques ne sont pas respectées et continuent de financer des sites d'information signalés ouvertement comme vecteurs de désinformation: https://disinformationindex.org/2021/02/ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/. Une étude menée par Avaaz en août 2020 a montré que le contenu des 10 principaux sites web diffusant des éléments de mésinformation sur la santé a été vu presque quatre fois plus sur Facebook que le contenu équivalent des sites web des 10 institutions de santé les plus importantes: https://secure.avaaz.org/campaign/en/facebook_threat_health/.

[18]Le plan d'action pour la démocratie européenne définit la mésinformation comme suit: *«on entend par "mésinformation" des contenus faux ou trompeurs transmis sans intention de nuire, même si leurs effets peuvent néanmoins être préjudiciables; c'est notamment le cas lorsque des personnes partagent de bonne foi de fausses informations avec des amis ou des membres de leur famille».*

[19]Le plan d'action pour la démocratie européenne définit la désinformation comme suit: *«on entend par "désinformation" des contenus faux ou trompeurs diffusés avec l'intention de tromper ou dans un but lucratif ou politique et susceptibles de causer un préjudice public».*

Pour en faciliter la lecture, les présentes orientations utilisent le terme général de «désinformation» pour désigner les différents phénomènes qu'il convient d'aborder, tout en reconnaissant clairement les différences importantes qui existent entre eux[20]. La désinformation dans ce sens comprend la désinformation au sens strict, la mésinformation, ainsi que les opérations d'influence[21] et l'ingérence étrangère[22] dans l'espace de l'information, notamment de la part d'acteurs étrangers, lorsque la manipulation de l'information a pour effet de causer un préjudice public important.

3.3 Une participation plus large

Les signataires du code actuel comprennent les principales plateformes en ligne opérant au sein de l'Union. Toutefois, une participation plus large des plateformes anciennes et nouvelles pourrait apporter une réponse plus complète et coordonnée face à la propagation de la désinformation. Parmi les nouveaux signataires potentiels peuvent figurer les fournisseurs de services en ligne qui diffusent des informations au public, tels que les réseaux sociaux ou les services de recherche plus petits (par exemple, les acteurs qui proposent des services spécialisés/thématiques ou au niveau national ou régional). Compte tenu des exigences pertinentes de mise en conformité, notamment les obligations en matière de rapports, les engagements pris dans le cadre du code renforcé devraient tenir compte de l'ampleur des services des signataires. Alors que les très grandes plateformes en ligne devront prendre des mesures fortes afin de faire face aux risques systémiques pertinents dans le cadre la proposition relative à la législation sur les services numériques, les mesures applicables aux services plus petits ou nouveaux ne devraient pas imposer de charge disproportionnée à leur égard.

Les services de messagerie privée peuvent également être utilisés de manière abusive pour alimenter la désinformation et la mésinformation, ainsi que cela a été observé lors des récentes campagnes électorales et pendant la pandémie de COVID-19[23]. Les fournisseurs de ces services pourraient être signataires du code et s'engager à prendre des mesures spécifiques adaptées à ce type de services, sans affaiblir le chiffrement souvent utilisé par ce type de services, et en tenant dûment compte de la protection de la vie privée et du droit à la vie privée et familiale, notamment pour les communications.

Afin d'accroître l'incidence du code sur la démonétisation de la désinformation, une participation plus large des parties prenantes de l'écosystème de la publicité au-delà du cercle des signataires actuels du code (associations européennes et nationales du secteur de la publicité) est essentielle. Le code bénéficierait en particulier d'une plus grande participation des marques (notamment celles dont les dépenses en matière de publicité en ligne sont importantes) ainsi que d'autres parties prenantes du secteur de la publicité en ligne (par exemple, les bourses d'annonces, les fournisseurs de technologies

---

[20]Le cas échéant, les présentes orientations établissent une distinction entre les différentes sous-catégories.

[21]Tel que défini dans le plan d'action pour la démocratie européenne: «*on entend par "opérations d'influence" les efforts coordonnés déployés par des acteurs nationaux ou étrangers pour influencer un public cible au moyen d'une série de moyens fallacieux, notamment la suppression de sources d'information indépendantes combinée à de la désinformation*».

[22]Tel que défini dans le plan d'action pour la démocratie européenne: «*on entend par "ingérences étrangères dans l'espace de l'information" (qui ont souvent lieu dans le cadre d'une opération hybride plus large), des efforts coercitifs et trompeurs déployés par un acteur d'un État étranger ou des agents de celui-ci dans le but d'entraver la formation et l'expression libres de la volonté politique des individus*».

[23]«Stop the virus of disinformation» (Arrêter le virus de la désinformation), Institut interrégional de recherche des Nations unies sur la criminalité et la justice (UNICRI), http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf

publicitaires, les agences de communication) et d'autres acteurs fournissant des services susceptibles d'être utilisés pour monétiser la désinformation (par exemple, les services de paiement électronique, les plateformes de commerce électronique, les systèmes de financement participatif et de dons)[24].

Parmi les nouveaux signataires pourraient aussi figurer d'autres parties prenantes susceptibles d'avoir une incidence importante par l'intermédiaire de leurs outils, de leurs instruments, de leurs solutions ou de leur expertise spécifique pertinente, notamment les vérificateurs de faits, les organisations fournissant des évaluations concernant les sites de désinformation ou évaluant la désinformation, ainsi que les prestataires de solutions technologiques susceptibles de soutenir les efforts de lutte contre la désinformation. Ces organisations peuvent contribuer dans une large mesure à la mise en œuvre efficace du code et à sa réussite.

3.4 Des engagements sur mesure

Afin de faciliter une participation plus large, le code renforcé devrait comprendre des engagements adaptés qui correspondent à la diversité des services fournis par les signataires et au rôle spécifique qu'ils jouent au sein de l'écosystème.

Les signataires devraient souscrire aux engagements qui sont pertinents pour leurs services. Bien que la participation au code et la souscription à ses engagements restent volontaires, afin de garantir l'efficacité du code en tant qu'outil permettant de réduire les risques, les signataires ne devraient pas, en principe, se soustraire aux engagements qui sont pertinents pour leurs services. Lorsqu'un signataire choisit de ne pas souscrire à un engagement donné pertinent pour son service, il devrait justifier sa position publiquement, dans l'esprit du considérant 68 de la proposition relative à la législation sur les services numériques. Les signataires qui fournissent des outils, des instruments ou des solutions visant à lutter contre la désinformation pourraient souscrire aux engagements appropriés et utiliser leur expertise pour soutenir les autres signataires du code. Toute exigence en matière de rapports pour ces organisations devrait être adaptée à leur mission.

3.5 L'Observatoire européen des médias numériques

Afin de contribuer efficacement à la lutte contre la désinformation, il est essentiel de bénéficier du soutien d'une communauté pluridisciplinaire comprenant des vérificateurs de faits, des chercheurs universitaires et d'autres acteurs pertinents. L'Observatoire européen des médias numériques (EDMO)[25] a été créé afin de contribuer à la création d'une telle communauté et de faciliter son travail. En apportant un soutien aux vérificateurs de faits et chercheurs indépendants, l'EDMO et ses pôles nationaux les aideront à mieux repérer et analyser les campagnes de désinformation. L'EDMO peut jouer un rôle important pour réaliser plusieurs des objectifs du code. Il est donc attendu des signataires du code qu'ils coopèrent avec l'EDMO, le cas échéant.

---

[24] «How COVID-19 conspiracists and extremists use crowdfunding platforms to fund their activities» (Les façons dont les conspirationnistes et les extrémistes du domaine de la COVID-19 utilisent les plateformes de financement participatif pour financer leurs activités), EUDisinfoLab https://www.disinfo.eu/publications/how-covid-19-conspiracists-and-extremists-use-crowdfunding-platforms-to-fund-their-activities/

[25] https://edmo.eu/

3.6 Un système d'alerte rapide

Comme le souligne le plan d'action contre la désinformation de 2018[26], les plateformes en ligne devraient coopérer avec le système d'alerte rapide de l'Union qui relie tous les États membres de l'Union et les institutions de l'Union concernées pour permettre des réponses conjointes à la désinformation en partageant des informations et en signalant en temps utile les campagnes de désinformation. Sur cette base, le code renforcé devrait examiner les possibilités de renforcer cette coopération, notamment en facilitant les échanges informels entre les signataires pour qu'ils présentent leurs travaux et leurs conclusions, et pour garantir des relations étroites, harmonisées et cohérentes au niveau national entre tous les États membres et les signataires, le cas échéant. Le code renforcé devrait également tenir compte de la coopération avec l'EDMO, tel que mentionné ci-dessus.

4 LE CONTROLE DES PLACEMENTS DE PUBLICITE

Comme expliqué, une action décisive visant à démonétiser les vecteurs de désinformation est essentielle à la réussite du code. Les engagements du code renforcé devraient donc prendre des mesures plus détaillées et adaptées pour traiter les risques de désinformation liés à la diffusion de publicités en ligne, en gardant à l'esprit les exigences réglementaires à venir dans la proposition relative à la législation sur les services numériques, qui s'appliquent à toutes les publicités en ligne, y compris la publicité à caractère politique et la publicité engagée et, le cas échéant, l'initiative annoncée relative à la publicité à caractère politique.

4.1 Démonétiser la désinformation

Le code devrait renforcer les engagements visant à démonétiser la diffusion d'éléments de désinformation sur les services des signataires ou sur les sites web de tiers[27]. Afin d'améliorer la transparence et l'obligation de rendre compte en ce qui concerne les placements publicitaires, les signataires participant à ces placements, notamment les entreprises de technologie publicitaire[28], devraient définir les critères qu'ils utilisent pour placer les publicités et adopter des mesures permettant de vérifier où sont diffusées les publicités, afin d'éviter qu'elles ne soient placées à proximité de contenus de désinformation ou sur des sites connus pour publier des éléments de désinformation de façon répétée. Les plateformes doivent s'engager, en particulier, à renforcer les conditions d'éligibilité et les processus d'examen des contenus pour les programmes de monétisation de contenus et de partage des revenus publicitaires sur leurs services, afin d'interdire la participation d'acteurs qui publient systématiquement des contenus bien connus pour véhiculer des éléments de désinformation[29]. En outre, les plateformes devraient également s'engager à renforcer les politiques pertinentes et à faire preuve de

---

[26]JOIN (2018) 36 final.

[27]Il est également prouvé que les recettes des publicités en ligne contribuent toujours de manière significative à la monétisation des sites de désinformation, notamment les publicités de grandes marques placées involontairement à proximité de contenus de désinformation. Par exemple, l'indice mondial de la désinformation estime que les sites de désinformation ciblant l'Europe engrangent près de 76 millions de dollars par an de recettes publicitaires: https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/.

[28]Un nombre limité d'entreprises de technologie publicitaire ont déjà adopté de telles politiques.

[29]Voir par exemple le rapport d'Avaaz de 2020 intitulé: «Why is YouTube Broadcasting Climate Misinformation to Millions?» (Pourquoi YouTube diffuse-t-il de fausses informations sur le climat à des millions de personnes?): https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/.

diligence afin d'exclure la participation aux réseaux publicitaires ou aux bourses d'annonces des sites web qui diffusent de manière constante des contenus de désinformation.

Les engagements dans ce domaine devraient également s'appuyer sur les outils de sécurité des marques et en améliorer la disponibilité et l'utilisation. Ces outils devraient intégrer des informations et des analyses provenant de vérificateurs de faits, de chercheurs et d'autres acteurs pertinents fournissant des informations, par exemple sur les sources des campagnes de désinformation. En bénéficiant de ces informations et de ces outils, les propriétaires de marques et les autres annonceurs devraient s'engager à tout mettre en œuvre pour éviter de placer leurs publicités à proximité de contenus de désinformation ou sur des sites qui publient des éléments de désinformation de façon répétée.

4.2 Améliorer la coopération entre les acteurs concernés

Afin d'obtenir des résultats tangibles, il est nécessaire que les différents acteurs de l'écosystème de la publicité coopèrent étroitement. À cette fin, comme indiqué à la section 3.3, une participation plus large des parties prenantes de l'écosystème de la publicité est essentielle. Le code renforcé devrait fournir un cadre pour élargir cette participation, qui renforcerait la coopération de tous les acteurs concernés et faciliterait davantage les initiatives intersectorielles en cours dans ce domaine[30].

Dans le cadre du code renforcé, tous les acteurs participant à l'achat, à la vente et au placement de publicité numérique devraient s'engager à échanger les bonnes pratiques et à renforcer la coopération. Cette coopération devrait faciliter l'intégration et le flux d'informations tout au long de la chaîne de valeur publicitaire, en particulier les informations pertinentes pour déterminer les vecteurs de désinformation dans le plein respect de toutes les règles pertinentes en matière de protection des données.

La coopération entre plateformes pourrait également comprendre l'échange d'informations sur les publicités constitutives de désinformation qu'une plateforme a refusées afin d'empêcher qu'elles ne s'affichent sur d'autres plateformes – par exemple, en créant un référentiel commun des publicités refusées – dans le but de sensibiliser les autres plateformes dont les services peuvent également être affectés.

Il convient d'élargir les actions visant à démonétiser la désinformation en faisant participer des acteurs actifs dans la chaîne de valeur de la monétisation en ligne, tels que les services de paiement électronique en ligne, les plateformes de commerce électronique et les systèmes pertinents de financement participatif et de dons.

---

[30]L'Alliance mondiale pour les médias responsables, lancée en juin 2019 sous les auspices de la Fédération mondiale des annonceurs (FMA), regroupe des plateformes et des acteurs du secteur publicitaire signataires du code, ainsi que d'autres parties prenantes éminentes de l'écosystème de la publicité. Elle travaille à l'élaboration d'un ensemble de définitions et de normes communes à l'ensemble du secteur concernant la manière dont les contenus préjudiciables sont classés sur les plateformes. Ces définitions et ces normes sont approuvées par les annonceurs et mises en œuvre par les plateformes dans leurs produits publicitaires et leurs outils de sécurité des marques. L'alliance cherche notamment à inclure dans cet ensemble une catégorie distincte relative à la désinformation et à la mésinformation. Voir le rapport de la FMA intitulé «Interim Report on Activities related to the EU Code of Practice on Disinformation» (Rapport intermédiaire sur les activités liées au code de bonnes pratiques de l'UE contre la désinformation), septembre 2020, p. 2: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69683

4.3 Engagements relatifs à la lutte contre les publicités contenant des éléments de désinformation

Dans le cadre du code renforcé, les signataires devraient s'engager à concevoir des politiques appropriées et adaptées concernant la publicité, qui s'attaquent à l'utilisation abusive de leurs systèmes publicitaires en vue de propager des éléments de désinformation[31]. Ils devraient faire appliquer ces politiques de manière cohérente et efficace. À cette fin, les signataires devraient coopérer avec les vérificateurs de faits afin de recenser les publicités contenant des éléments de désinformation qui ont été vérifiées et démenties. Pour garantir la cohérence de la mise en œuvre, les signataires devraient s'engager à adapter leurs systèmes actuels de vérification et d'examen des publicités pour faire en sorte que les publicités placées sur leurs services ou au moyen de ceux-ci respectent leurs politiques en matière de publicité concernant la désinformation. Les signataires devraient aussi s'engager à expliquer clairement aux annonceurs quelles politiques en matière de publicité n'ont pas été respectées lorsqu'ils refusent ou suppriment des publicités constitutives de désinformation ou désactivent des comptes publicitaires[32].

5 PUBLICITE A CARACTERE POLITIQUE ET PUBLICITE ENGAGEE

La «publicité à caractère politique» et la «publicité engagée»[33] jouent un rôle important dans l'organisation des campagnes politiques et des débats publics concernant les grands enjeux sociétaux. Ces contenus payants en ligne peuvent jouer un rôle décisif pour former l'opinion publique et influencer le résultat des élections. L'organisation des élections dans l'UE est largement réglementée au niveau des États membres. En effet, diverses règles pertinentes concernent la publicité à caractère politique, notamment sa transparence. Dans le plan d'action pour la démocratie européenne, la Commission a annoncé une législation visant à renforcer la transparence de la publicité à caractère politique. Afin de garantir un niveau adéquat de transparence et d'obligation de rendre compte dans ce domaine, il y a lieu de renforcer davantage les engagements du code, en vue de soutenir le cadre juridique plus large.

La révision du code dans ce domaine devra tenir compte de la proposition législative à venir de la Commission sur la transparence du contenu politique sponsorisé et des dispositions pertinentes de la proposition relative à la législation sur les services numériques. Un code renforcé constituera un vecteur important pour réaliser des progrès tangibles en vue de soutenir le cadre juridique existant, pour ouvrir la voie à un renforcement de la législation, par l'intermédiaire du nouveau cadre législatif lorsqu'il

---

[31]Divers éléments montrent que des publicités en ligne contenant des éléments de désinformation que les vérificateurs de faits ont repérées et démenties demeurent en place. Voir «Facebook Approved Ads With Coronavirus Misinformation» (Facebook a approuvé des publicités contenant de fausses informations sur le coronavirus): https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/.

[32]Comme l'a noté la Commission, les politiques des plateformes poursuivent une série d'objectifs, dont certains ne sont pas spécifiquement adaptés à la lutte contre la désinformation, par exemple, les allégations commerciales sans fondement, les pratiques commerciales trompeuses. Voir document SWD (2020) 180 final.

[33]Bien qu'il n'existe actuellement dans le code aucune définition commune de la publicité engagée, un consensus semble se dégager sur le fait qu'il s'agit de publicités qui intègrent du contenu sponsorisé sur des questions de société ou liées à un débat d'intérêt général qui pourraient influencer le débat public. Le changement climatique, les questions liées à l'environnement, l'immigration ou la COVID-19 sont des exemples de telles questions.

sera mis en place, et pour concevoir des solutions pilotées par le secteur des entreprises en vue de soutenir sa mise en œuvre et de réaliser des progrès constants dans ce domaine.

Afin que les engagements soient appliqués de manière cohérente et efficace, il est nécessaire que les signataires aient une définition commune de la «publicité à caractère politique» et de la «publicité engagée» qui tienne compte de manière adéquate des cadres juridiques nationaux en vigueur. Les signataires doivent s'assurer qu'ils se conforment aux lois en vigueur et qu'ils alignent leurs pratiques sur la législation à venir relative à la transparence du contenu politique sponsorisé.

5.1 Marquage efficace des publicités à caractère politique et des publicités engagées

Le code devrait inclure des engagements renforcés garantissant la transparence et la diffusion publique des publicités à caractère politique et des publicités engagées, en tenant compte des dispositions pertinentes de la proposition relative à la législation sur les services numériques[34], de l'initiative législative à venir concernant la transparence de la publicité à caractère politique, et sans préjudice des cadres réglementaires existants. Ces publicités devraient faire l'objet d'un marquage clair et efficace et il devrait être possible de repérer qu'il s'agit d'un contenu payant. Les utilisateurs devraient être en mesure de comprendre que le contenu affiché comporte des publicités liées à des enjeux politiques ou sociétaux. Le code renforcé pourrait inclure un ensemble de critères et d'exemples communs concernant le repérage et le marquage des publicités à caractère politique et des publicités engagées. Le cas échéant, les signataires devraient intégrer des recherches pertinentes afin d'améliorer l'efficacité des marquages en vue d'informer les utilisateurs[35]. Le code devrait inclure des engagements visant à garantir que les marquages restent en place lorsque les utilisateurs partagent de manière organique[36] des publicités à caractère politique ou des publicités engagés, afin qu'elles soient toujours clairement repérées en tant que publicités.

5.2 Engagements en matière de vérification et de transparence des publicités à caractère politique et des publicités engagées

Les signataires qui affichent des publicités à caractère politique et des publicités engagées devraient s'assurer que les utilisateurs puissent voir l'identité de l'annonceur, et devraient prendre un engagement spécifique définissant les obligations de transparence conformément aux exigences de la proposition relative à la législation sur les services numériques[37].

Les signataires devraient également faire des efforts raisonnables en vue de s'assurer, au moyen de systèmes efficaces de vérification de l'identité et d'autorisation, que toutes les conditions nécessaires sont remplies avant d'autoriser le placement de ces types d'annonces.

---

[34]En particulier, l'article 24.

[35]Dobber et al., «Effectiveness of online political ad disclosure labels: empirical findings» (Efficacité des marquages relatifs aux publicités en ligne à caractère politique: résultats empiriques), mars 2021: https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-discloures-experiment_update.pdf.

[36]On entend par «contenu organique» le contenu gratuit que les utilisateurs partagent entre eux sans payer. Cela comprend également les situations dans lesquelles les utilisateurs partagent entre eux du contenu sponsorisé qui devient alors du contenu organique.

[37]Proposition relative à la législation sur les services numériques, article 30.

5.3 Transparence des plateformes de messagerie

Le code de bonnes pratiques révisé devrait intégrer de nouveaux engagements adaptés concernant l'utilisation des plateformes de messagerie pour la diffusion de publicités à caractère politique et de publicités engagées, dans le plein respect du règlement général sur la protection des données (RGPD) et des exigences de l'UE en matière de respect de la vie privée concernant les services de communications électroniques. L'exigence susmentionnée selon laquelle, lorsque des utilisateurs partagent du contenu politique sponsorisé, ce dernier doit continuer à être marqué comme contenu payant, doit également s'appliquer, dans la mesure du possible, au contenu politique sponsorisé partagé sur les plateformes de messagerie. À cette fin, les signataires devraient mettre au point des solutions compatibles avec la technologie de chiffrement souvent utilisée par les plateformes de messagerie, sans affaiblir ce chiffrement d'aucune manière.

5.4 Ciblage des publicités à caractère politique

Le microciblage de la publicité à caractère politique peut susciter diverses préoccupations, notamment en ce qui concerne la conformité aux règles de protection des données, car le microciblage repose sur des informations à caractère personnel et intègre parfois des techniques sophistiquées de profilage psychologique[38]. Il peut affecter le droit des électeurs à recevoir des informations, puisqu'il permet aux annonceurs politiques d'envoyer des messages personnalisés à des publics ciblés, tandis que les autres publics peuvent être privés de ces informations. Le microciblage complique la vérification des faits ou l'examen de ces publicités, ainsi que la possibilité pour les individus de faire valoir leurs droits, notamment en matière de protection des données. Cela peut accroître le risque de polarisation politique[39].

Le code renforcé devrait contribuer à limiter ou à éviter les risques liés au microciblage des personnes par la publicité à caractère politique et/ou la publicité engagée À cet égard, il convient de garantir le plein respect du RGPD et des autres lois pertinentes, en particulier l'obtention d'un consentement valide le cas échéant[40]. L'accès à l'information devrait être facilité afin de permettre aux autorités compétentes d'exercer leurs fonctions de surveillance et d'application de la loi.

Les signataires devraient s'engager à faire en sorte que les citoyens soient clairement informés lorsqu'ils font l'objet d'un microciblage et qu'ils reçoivent des informations utiles sur les critères et les données utilisés à cette fin. Ils devraient mettre en œuvre des mesures de transparence fortes dans ce domaine, notamment des bibliothèques de

---

[38]Les propositions de législation sur les services numériques et de législation sur les marchés numériques comportent des obligations spécifiques en matière de transparence.

[39]Voir, par exemple, Papakyriakopoulos et. al, «Social media and microtargeting: Political data processing and the consequences for Germany» (Réseaux sociaux et microciblage: le traitement des données politiques et ses conséquences pour l'Allemagne), Big Data & Society, novembre 2018, doi 10.1177/2053951718811844, ou Lewandowsky et al., «Understanding the influence of online technologies on political behaviour and decision-making» (Comprendre l'influence des technologies en ligne sur le comportement et la prise de décision politiques), EUR 30422 EN, Office des publications de l'Union européenne, Luxembourg.

[40]Pour obtenir de plus amples informations, voir les lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679 et les lignes directrices 08/2020 sur le ciblage des utilisateurs des médias sociaux du comité européen de la protection des données (qui fournissent des exemples de cas où le consentement est requis pour la publicité ciblée).

publicités dédiées et consultables contenant toutes les publicités microciblées diffusées auprès de groupes d'utilisateurs spécifiques[41], accompagnées d'informations sur les critères de ciblage et de diffusion.

5.5 Amélioration des registres de publicités et fonctionnalités minimales pour les interfaces de programmation (API)

Le code renforcé devrait garantir que les plateformes signataires s'engagent à améliorer l'exhaustivité et la qualité des informations contenues dans leurs registres de publicités à caractère politique, afin que ceux-ci contiennent effectivement tous les contenus politiques sponsorisés qui ont été diffusés. Ces registres devraient fournir des informations actuelles et régulièrement mises à jour concernant le volume et le budget des publicités à caractère politique diffusées par les annonceurs politiques dans les États membres, le nombre de fois où chaque publicité a été affichée en ligne et les critères de ciblage utilisés par l'annonceur, en tenant compte des dispositions pertinentes de la proposition relative à la législation sur les services numériques et de la proposition législative à venir concernant la publicité à caractère politique[42].

Certaines plateformes ont développé des interfaces de programmation (API) ou d'autres interfaces permettant aux utilisateurs et aux chercheurs d'effectuer des recherches personnalisées dans leurs registres de publicités à caractère politique. Les fonctionnalités de ces API sont toutefois très limitées. Le code renforcé devrait garantir que les API relatives aux registres des publicités à caractère politique des plateformes comportent un ensemble de fonctionnalités minimales, ainsi qu'un ensemble de critères de recherche minimaux permettant aux utilisateurs et aux chercheurs d'effectuer des recherches personnalisées afin d'extraire des données en temps réel dans des formats normalisés et de faciliter la comparaison, la recherche et le suivi entre plateformes. Si des registres relatifs à des publicités engagées sont mis en place, leurs API devraient présenter des fonctionnalités et des possibilités de recherche comparables. Les engagements devraient également garantir un large accès aux API et faire en sorte que les fonctionnalités des API soient régulièrement mises à jour afin de répondre aux besoins des chercheurs.

6 INTEGRITE DES SERVICES

Le code renforcé devrait prévoir une couverture complète des formes nouvelles et existantes de comportements manipulateurs utilisés pour propager des éléments de désinformation. Il devrait tenir compte du caractère évolutif de la propagation des éléments de désinformation et des risques plus larges qui y sont associés, par exemple le fait que les campagnes de désinformation peuvent faire partie de menaces hybrides pour la sécurité, en particulier lorsqu'elles sont associées à des cyberattaques[43]. Il devrait inclure des engagements adaptés visant à remédier aux vulnérabilités et à garantir la transparence et l'obligation de rendre compte des mesures que prennent les signataires en vue de limiter les comportements manipulateurs qui, selon leurs conditions d'utilisation pertinentes, ne sont pas autorisés sur les services des signataires, compte tenu également

[41]Par exemple, si les bibliothèques de publicités comportent les données nécessaires, elles peuvent permettre de vérifier en ligne si la durée d'exposition aux messages politiques est la même.
[42]Voir proposition relative à la législation sur les services numériques, article 30.
[43]Communication conjointe intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides», [JOIN(2018) 16 final]

des exigences réglementaires à venir énoncées dans la proposition relative à la législation sur les services numériques[44].

6.1 Interprétation commune des comportements manipulateurs interdits

Afin de garantir une approche cohérente, le code renforcé devrait garantir que les signataires s'accordent sur une interprétation commune des comportements manipulateurs interdits sur leurs services, notamment les «comportements non authentiques», sans préjudice des législations nationales et de l'UE existantes. Cette interprétation devrait être suffisamment large pour couvrir l'ensemble des comportements par lesquels des acteurs malveillants peuvent tenter de manipuler des services. À cette fin, les signataires devraient dresser une liste exhaustive des tactiques, techniques et procédures de manipulation qui constituent un comportement non authentique interdit sur leurs services. Les techniques recensées devraient être suffisamment définies pour permettre de comparer la prévalence, sur les différentes plateformes, des comportements interdits et de déterminer l'efficacité des mesures prises pour y remédier. Cette interprétation commune devrait fournir aux signataires, aux régulateurs, à la société civile et aux autres parties prenantes un vocabulaire commun leur permettant de discuter des problèmes de la désinformation et de la manipulation en ligne, tant dans le contexte du code de bonnes pratiques que dans d'autres enceintes, telles que le système d'alerte rapide de l'UE et le réseau de coopération électorale, en préparation de l'application de la proposition relative à la législation sur les services numériques. Ces travaux devraient tenir compte de l'évolution rapide de la situation concernant les tactiques, techniques et procédures de manipulation et refléter ces changements éventuels lors de l'élaboration de la terminologie et des définitions.

6.2 Engagements renforcés visant à limiter les comportements manipulateurs interdits

Le code renforcé devrait énoncer de nouveaux engagements relatifs aux comportements manipulateurs interdits, couvrant tout l'éventail des techniques de manipulation et exigeant des réponses efficaces pour y remédier. Ces engagements devraient exiger des signataires qu'ils luttent contre les techniques de manipulation en constante évolution, telles que les opérations de piratage et de divulgation («hack and leak»), le piratage de comptes, la création de groupes non authentiques, l'usurpation d'identité, les trucages vidéo ultra-réalistes, l'achat de faux engagements ou la participation obscure d'influenceurs. En outre, les engagements ne devraient pas seulement exiger des signataires qu'ils publient des politiques pertinentes, mais ils devraient également définir des éléments, des objectifs et des critères de référence de base concernant les mesures déployées afin de lutter contre les comportements manipulateurs interdits. Le code renforcé devrait prendre en considération les obligations de transparence pour les systèmes d'intelligence artificielle (IA) qui génèrent ou manipulent du contenu et la liste des pratiques de manipulation interdites par la proposition de législation relative à l'intelligence artificielle[45].

[44]D'après l'article 26, paragraphe 1, point c), de la proposition relative à la législation sur les services numériques, la «manipulation intentionnelle» des services constitue un risque systémique, contre lequel les très grandes plateformes doivent prendre des mesures d'atténuation des risques.
[45]COM (2021) 206 final.

6.3 Ajustement des engagements, coopération et transparence

Afin de garantir la pertinence et l'adéquation permanentes du code renforcé, celui-ci devrait instaurer un mécanisme permettant d'ajuster ses engagements au fil du temps, en fonction des éléments probants les plus récents sur les comportements et les tactiques, techniques et procédures de manipulation que les acteurs malveillants emploient.

Les signataires devraient s'engager à mettre en place des canaux d'échange entre leurs équipes respectives chargées de la confiance, de la cybersécurité et de la sécurité. Ces canaux d'échange devraient faciliter le partage proactif d'informations sur les opérations d'influence et les ingérences étrangères dans l'espace de l'information sur les services des signataires afin de prévenir la résurgence de telles campagnes sur d'autres plateformes. Les résultats et les enseignements tirés devraient être intégrés dans les rapports de suivi annuels des signataires, être abordés au sein du groupe de travail permanent[46] et être mis à disposition régulièrement dans des formats de données courants[47].

Les engagements garantissent que toutes les politiques et mesures sont clairement communiquées aux utilisateurs, y compris par l'intermédiaire du centre de transparence[48]. Les signataires devraient également s'engager à transmettre toutes les actions contre les comportements manipulateurs interdits à un système interne de traitement des réclamations, en tenant compte des dispositions pertinentes de la proposition relative à la législation sur les services numériques[49].

7 DONNER LES MOYENS D'AGIR AUX UTILISATEURS

Afin de limiter l'incidence de la désinformation, il est essentiel de donner les moyens d'agir aux utilisateurs. Une meilleure compréhension du fonctionnement des services en ligne ainsi que des outils qui favorisent un comportement plus responsable en ligne ou qui permettent aux utilisateurs de déceler et de signaler des contenus faux et/ou trompeurs peuvent limiter considérablement la propagation des éléments de désinformation. Les engagements du code dans ce domaine devraient être enrichis de manière à couvrir un large éventail de services, y compris par exemple des engagements adaptés aux services de messagerie. Ils devraient également inclure des mécanismes de recours contre les mesures prises par les signataires après les signalements des utilisateurs. Les signataires devraient également prendre expressément en considération la situation des enfants qui peuvent être particulièrement vulnérables face à la désinformation.

7.1 Engagement à prendre des mesures visant à améliorer l'éducation aux médias

Plusieurs signataires ont fait des efforts dans le domaine de l'éducation aux médias en fournissant des outils pertinents aux utilisateurs. Dans le cadre du code renforcé, les

[46]En ce qui concerne le groupe de travail permanent, voir la section 9.2.3ci-après.
[47]En tenant également compte du cadre AMITT (Adversarial Misinformation and Influence Tactics and Techniques – (Tactiques et techniques de mésinformation et d'influence antagonistes): https://cogsec-collab.org/
[48]En ce qui concerne le centre de transparence, voir la section 9.2.2ci-après.
[49]Notamment l'article 17 qui s'applique déjà aux décisions incompatibles avec leurs conditions générales, notamment les décisions de retirer des contenus ou de rendre l'accès à ceux-ci impossible, les décisions de suspendre ou de résilier, entièrement ou partiellement, la fourniture du service aux bénéficiaires ou les décisions de suspendre ou de résilier le compte des bénéficiaires.

signataires devraient s'engager à poursuivre ces efforts et, en particulier, à faire davantage participer la communauté de l'éducation aux médias à la conception et à la mise en œuvre des outils ainsi qu'à l'évaluation des campagnes d'éducation aux médias sur leurs services, notamment pour protéger les enfants. Ces efforts pourraient également être alignés sur les initiatives de la Commission dans le domaine de l'éducation aux médias[50], notamment le nouveau plan d'action en matière d'éducation numérique 2021-2027[51], afin de tirer parti des synergies pertinentes. À cette fin, le groupe d'experts sur l'éducation aux médias de la Commission[52] et l'EDMO peuvent apporter leur soutien afin d'instaurer un cadre permanent de discussion.

7.2 Engagement en faveur d'une «conception sûre»

La conception et l'architecture des services en ligne ont une incidence importante sur le comportement des utilisateurs[53]. Les signataires devraient donc s'engager à évaluer les risques que présentent leurs systèmes et à concevoir l'architecture de leurs services de manière à réduire le plus possible les risques liés[54] à la propagation et à l'amplification de la désinformation[55]. Cela pourrait également inclure des essais préalables de l'architecture des systèmes. Les signataires devraient également investir dans la recherche et mettre au point des caractéristiques et des conceptions de produits qui favorisent la pensée critique des utilisateurs ainsi que l'utilisation responsable et sûre de leurs services.

Les plateformes en ligne pourraient également collaborer avec les prestataires de solutions technologiques pour intégrer dans leurs services des solutions permettant de vérifier l'authenticité ou l'exactitude des contenus numériques ou d'en déterminer la provenance ou la source[56].

---

[50]Voir en particulier les actions définies dans le plan d'action pour la démocratie européenne, [COM (2020) 790 final] et le plan d'action pour les médias et l'audiovisuel [COM (2020) 784 final].

[51]Le plan d'action en matière d'éducation numérique [COM (2020) 624 final] propose d'élaborer des lignes directrices à l'intention des enseignants et des formateurs en vue de lutter contre la désinformation et de promouvoir la culture numérique par l'éducation et la formation.

[52]https://digital-strategy.ec.europa.eu/en/policies/media-literacy

[53]Voir, par exemple, Lewandowsky et al., «Understanding the influence of online technologies on political behaviour and decision-making» (Comprendre l'influence des technologies en ligne sur le comportement et la prise de décision politiques), EUR 30422 EN, Publications Office des publications de l'Union européenne, Luxembourg, 2020.

[54]Voir proposition relative à la législation sur les services numériques, article 26, paragraphe 1, point c), sur l'évaluation des risques connexes.

[55]Des interventions techniques simples (par exemple, des messages «pop-up» demandant aux utilisateurs s'ils souhaitent vraiment partager des liens qu'ils n'ont pas consultés) peuvent inciter les utilisateurs à examiner le contenu avant de le diffuser et contribuer ainsi à limiter la propagation d'informations fausses et/ou trompeuses par des utilisateurs de bonne foi. Exemples: Le message «Pensez à vérifier avant de tweeter» mis en œuvre par Twitter: https://help.twitter.com/fr/using-twitter/how-to-retweet;
Les panneaux d'information «Fact-checking» de YouTube: https://support.google.com/youtube/answer/9229632?hl=fr; Un message contextuel sur Facebook avant le partage d'un contenu démenti par un vérificateur de faits: https://fr-fr.facebook.com/journalismproject/programs/third-party-fact-checking/faqs;
Outil «Know your Facts» de TikTok: https://newsroom.tiktok.com/en-gb/taking-action-against-covid-19-vaccine-misinformation.

[56]À la section 3.3des orientations, les parties prenantes qui peuvent, au moyen de leurs outils, instruments ou solutions contribuer à la lutte contre la désinformation, sont invitées à devenir de nouveaux signataires du code.

Les fournisseurs de systèmes en ligne fondés sur l'IA devraient également prendre en considération les dispositions pertinentes de la proposition de législation relative à l'intelligence artificielle.

7.3 Responsabilisation des systèmes de recommandation

En déterminant l'ordre dans lequel les informations sont présentées, les systèmes de recommandation ont une incidence significative sur les informations effectivement consultées par les utilisateurs. Il est primordial que les signataires du code renforcé s'engagent à faire en sorte que leurs systèmes de recommandation soient transparents pour ce qui est des critères utilisés pour accorder ou non la priorité aux informations, en donnant la possibilité aux utilisateurs de personnaliser les algorithmes de classement. Tout cela doit être fait en tenant dûment compte du principe de la liberté des médias et en prenant en considération les exigences des dispositions pertinentes de la proposition relative à la législation sur les services numériques[57].

Les engagements devraient également inclure des mesures concrètes visant à atténuer le risque que les systèmes de recommandation contribuent à la propagation virale d'éléments de désinformation, notamment la suppression des informations fausses et/ou trompeuses figurant dans les contenus recommandés lorsqu'elles ont été démenties par des vérificateurs de faits indépendants, ainsi que la suppression des pages web et l'exclusion des acteurs qui propagent de manière constante des éléments de désinformation.

7.4 Visibilité des informations fiables présentant un intérêt pour le public

La pandémie de COVID-19 a mis en lumière l'importance, en particulier en temps de crise, de promouvoir des informations fiables présentant un intérêt pour le public, notamment celles que fournissent les autorités sanitaires concernant les mesures de prévention de la maladie ou la sécurité des vaccins[58]. Les signataires ont mis en œuvre diverses solutions visant à fournir aux utilisateurs de telles informations et à les rendre visibles et facilement accessibles. En s'appuyant sur cette expérience, les signataires du code renforcé devraient s'engager à poursuivre le développement et l'application de ces outils spécifiques (par exemple, des panneaux d'information, des bannières, des fenêtres «pop-up», des cartes et des messages de guidage) qui accordent la priorité aux sources faisant autorité sur des sujets présentant un intérêt particulier pour le public et la société ou dans des situations de crise et qui mènent les utilisateurs à ces sources.

Afin d'approfondir l'engagement du code existant[59] concernant la hiérarchisation des contenus pertinents, authentiques et faisant autorité, les signataires devraient également s'engager à publier des informations décrivant la méthode employée par leurs systèmes de recommandation à cet égard. Ces informations devraient figurer dans le centre de transparence. Les signataires du code devraient envisager de garantir que ces informations peuvent être vérifiées par des tiers ou par un audit indépendant, en tenant

[57]Notamment les articles 26, 27 et 29

[58]Les rapports de suivi sur la COVID-19 fournissent des données sur le nombre de vues ou les taux de clics des panneaux et bannières d'information fournissant de telles informations: https://digital-strategy.ec.europa.eu/en/library/reports-march-actions-fighting-covid-19-disinformation-monitoring-programme

[59]Voir l'engagement nº 8 du code de bonnes pratiques contre la désinformation.

compte également des dispositions pertinentes de la proposition relative à la législation sur les services numériques.

7.5 Avertissements adressés aux utilisateurs qui interagissent ou ont interagi avec des contenus faux ou trompeurs

Il est essentiel de démentir les informations fausses et/ou trompeuses afin de freiner le phénomène de la désinformation[60]. Plusieurs signataires ont entamé une coopération avec des vérificateurs de faits indépendants et/ou ont mis en place des équipes de modération internes afin de marquer les contenus faux ou trompeurs. Toutefois, à l'heure actuelle, le code ne comporte pas d'engagements en la matière. En conséquence – en complément des nouveaux engagements visant à garantir la mise en pratique cohérente de la vérification des faits, comme indiqué à la section 8.3ci-après – les signataires devraient s'engager à fournir, pour toutes les langues de l'UE dans lesquelles leurs services sont fournis, des systèmes permettant de marquer régulièrement et de manière cohérente les contenus repérés comme étant faux ou trompeurs et d'avertir de façon ciblée les utilisateurs qui ont interagi avec ces contenus. Les signataires devraient s'engager à informer les utilisateurs des raisons pour lesquelles un contenu ou un compte spécifique a été marqué, rétrogradé dans le classement ou affecté d'une autre manière par les mesures prises, ainsi que les motifs de cette action. Les signataires devraient s'engager à concevoir leurs systèmes de marquage et d'avertissement conformément aux preuves scientifiques les plus récentes sur la manière de maximiser les effets de ces interventions, en veillant en particulier à ce qu'ils soient conçus de manière à capter l'attention des utilisateurs[61].

7.6 Fonctionnalité permettant de signaler les fausses informations préjudiciables

Même si certains signataires proposent déjà une fonctionnalité spécifique permettant aux utilisateurs de signaler les informations fausses et/ou trompeuses, elle n'est pas encore disponible sur tous les services. Le code renforcé devrait comporter un engagement spécifique exigeant des signataires concernés qu'ils offrent des procédures simples et efficaces sur leurs services, afin de permettre aux utilisateurs de signaler des éléments de désinformation susceptibles de causer un préjudice public ou individuel. Cette fonctionnalité devrait également prendre en charge les systèmes et mécanismes de marquage afin de faciliter le repérage de la résurgence de contenus faux déjà marqués comme tels dans d'autres langues ou sur d'autres services, dans le plein respect de la liberté d'expression. L'engagement devrait préciser que cette fonctionnalité doit être dûment protégée contre les abus (c'est-à-dire la tactique du «signalement de masse» pour faire taire les autres voix) et disponible dans toutes les langues des États membres de l'UE dans lesquelles les services sont fournis. Les mesures prises par les signataires concernant les contenus signalés devraient respecter la liberté d'expression et ne pas être disproportionnées. Parmi les mesures dans ce domaine pourrait figurer l'application d'une procédure transparente de vérification des faits pour le contenu signalé, avec des actions de suivi ultérieures, telles que le marquage du contenu, le cas échéant. Les signataires devraient s'engager à fournir aux utilisateurs des informations de suivi concernant le contenu signalé, en précisant par exemple s'il a fait l'objet d'un examen et, dans l'affirmative, les résultats de l'évaluation et toute mesure prise par rapport audit

[60]The Debunking Handbook 2020 (Le manuel des dénégations): https://sks.to/db2020.
[61]Les optimisations peuvent par exemple concerner l'aspect visuel, le moment ou la présentation graphique de l'intervention.

contenu. De même, les utilisateurs dont le contenu ou le compte a fait l'objet de telles mesures devraient être informés afin de comprendre les raisons des mesures prises à leur égard et avoir accès à un mécanisme approprié et transparent pour introduire un recours et demander réparation contre les mesures appliquées.

7.7 Disponibilité d'indicateurs permettant une navigation en ligne éclairée

Le code renforcé n'a pas pour objectif d'évaluer la véracité du contenu éditorial. Toutefois, compte tenu de l'abondance des informations disponibles en ligne, les utilisateurs sont confrontés à des difficultés pour déterminer les sources d'information qu'ils peuvent consulter et qui sont fiables. Les indicateurs de fiabilité, axés sur l'intégrité de la source, élaborés par des tiers indépendants, en collaboration avec les médias d'information, notamment les associations de journalistes et les organisations de défense de la liberté des médias, ainsi que les vérificateurs de faits, peuvent aider les utilisateurs à faire des choix éclairés[62].

Les signataires pourraient faciliter l'accès à ces indicateurs en donnant aux utilisateurs la possibilité de les utiliser sur leurs services. Dans ce cas, le code renforcé devrait garantir que les signataires assurent la transparence de ces indicateurs tiers, y compris en ce qui concerne la méthode utilisée.

La mise en œuvre de ces indicateurs de fiabilité devrait être pleinement conforme aux principes de liberté et de pluralisme des médias. À cette fin, il convient de laisser aux utilisateurs le soin de décider s'ils souhaitent utiliser de tels outils[63].

7.8 Mesures visant à freiner la désinformation dans les applications de messagerie

Outre les initiatives récentes mises au point en coopération avec des vérificateurs de faits[64], les signataires qui fournissent des applications de messagerie privée devraient tester et mettre en œuvre des fonctionnalités techniques aidant les utilisateurs à repérer les éléments de désinformation diffusés sur ces services. Ces solutions devraient être compatibles avec la nature de ces services et en particulier avec le droit à la confidentialité des communications, sans affaiblir le chiffrement d'aucune manière. Ces fonctionnalités pourraient, par exemple, aider les utilisateurs à contrôler si une vérification des faits a révélé le caractère faux d'un contenu particulier qu'ils reçoivent. Une telle vérification serait possible, par exemple, au moyen de solutions qui rendent visibles les marquages de vérification des faits lorsque le contenu des réseaux sociaux est diffusé sur une application de messagerie. Les signataires pourraient également envisager des solutions permettant aux utilisateurs de comparer les contenus qu'ils reçoivent sur une application de messagerie à une base répertoriant les vérifications de faits.

---

[62]Parmi les exemples de tels indicateurs, citons l'indice mondial de la désinformation, la Journalism Trust Initiative (JTI ou initiative pour la fiabilité de l'information) ou le Trust Project (projet en faveur de la fiabilité), ainsi que le service NewsGuard.

[63]Des outils permettant d'évaluer la fiabilité des sources d'information, tels que les «labels de confiance», devraient être mis à la disposition des utilisateurs qui pourraient les consulter s'ils le souhaitent. Les utilisateurs pourraient également avoir la possibilité d'intégrer des signaux relatifs à la fiabilité des sources médiatiques dans les systèmes automatisés qui sélectionnent et classent les contenus qui s'affichent dans leurs flux.

[64]Les organismes de vérification des faits, soutenus par certains fournisseurs d'applications de messagerie, permettent aux utilisateurs de ces applications de faire vérifier les faits des messages qu'ils ont reçus par l'intermédiaire de ces canaux privés: https://faq.whatsapp.com/general/ifcn-fact-checking-organizations-on-whatsapp/?lang=fr

8 DONNER LES MOYENS D'AGIR A LA COMMUNAUTE DES CHERCHEURS ET DES VERIFICATEURS DE FAITS

Compte tenu de leur contribution essentielle à une stratégie efficace de lutte contre la désinformation, le code renforcé devrait définir un cadre permettant à la communauté des chercheurs et des vérificateurs de faits d'avoir un accès fiable aux données de la plateforme et soutenir leurs activités de manière adéquate.

8.1 Accès aux données des signataires pour la recherche sur la désinformation

En proposant des analyses fondées sur des éléments factuels, les chercheurs sont essentiels à la bonne compréhension de l'évolution des risques liés à la désinformation[65] et peuvent contribuer à l'élaboration de mécanismes d'atténuation des risques. Pour ce travail, il est décisif de pouvoir accéder aux données de la plateforme. La proposition relative à la législation sur les services numériques prévoit un mécanisme réglementaire permettant aux chercheurs agréés d'accéder aux données afin de mener des recherches sur les risques découlant des services des plateformes[66]. Le code renforcé devrait créer un cadre qui, pendant la période transitoire avant l'adoption de la législation sur les services numériques, permette déjà aux chercheurs de bénéficier de l'accès nécessaire aux données des plateformes et qui facilite également à long terme l'élaboration d'un cadre spécifique d'accès aux données adapté à la recherche sur les phénomènes de la désinformation.

8.1.1 Cadre général pour l'accès aux données

En ce qui concerne le code renforcé, les signataires concernés, en particulier les plateformes, devraient s'engager à créer conjointement un cadre solide pour l'accès aux données à des fins de recherche. Les conditions d'accès devraient être transparentes, ouvertes et non discriminatoires, proportionnées et justifiées. En ce qui concerne les données à caractère personnel, les conditions doivent être conformes au RGPD. En général, les conditions d'accès aux données doivent respecter le droit à la confidentialité des communications et protéger de manière appropriée les droits et intérêts légitimes de toutes les parties concernées.

Les signataires devraient élaborer le cadre en coopération avec la communauté des chercheurs, l'EDMO et les autorités nationales compétentes. Les engagements devraient inclure un calendrier détaillé des progrès attendus en matière de conception et de mise en œuvre du cadre.

Le cadre devrait envisager différentes règles d'accès aux données, avec des garanties appropriées pour i) les données anonymisées et à caractère non personnel et pour ii) les données nécessitant un examen complémentaire, y compris les données à caractère personnel. Le cadre devrait prévoir la possibilité d'un accès en temps réel à certains types de données, afin de pouvoir évaluer rapidement les risques émergents ou évolutifs ainsi que la conception de mesures d'atténuation appropriées.

Pendant que le cadre est en cours d'élaboration, les signataires devraient mettre en place des solutions temporaires. Par exemple, l'utilisation d'«espaces d'expérimentation»

[65]Cet aspect est crucial pour informer les signataires, la Commission, les autorités nationales compétentes et le public.
[66]En particulier, l'article 31.

pourrait permettre à un nombre limité de chercheurs d'accéder à des données pertinentes de la plateforme à des fins de recherche sur des sujets spécifiques, afin d'éclairer la conception du cadre et de tester des solutions opérationnelles permettant un accès plus large aux données sur l'ensemble des plateformes.

8.1.2 Accès aux données anonymisées et à caractère non personnel

Le code renforcé devrait comporter un engagement à fournir, dans la mesure du possible, un accès continu, en temps réel, stable et harmonisé aux données anonymisées, agrégées ou à caractère non personnel à des fins de recherche, au moyen d'API ou d'autres solutions techniques ouvertes et accessibles permettant d'exploiter pleinement les ensembles de données.

Les solutions d'accès aux données devraient faciliter la recherche et l'analyse des données. Les signataires concernés devraient s'assurer que les fonctionnalités des systèmes d'accès répondent aux besoins des chercheurs et sont interopérables. Les engagements devraient prévoir des procédures permettant de signaler le dysfonctionnement des systèmes d'accès, de rétablir l'accès et de remédier aux fonctionnalités défaillantes dans un délai raisonnable.

8.1.3 Accès aux données nécessitant un examen complémentaire, y compris les données à caractère personnel

Les données susceptibles de divulguer des informations à caractère personnel, y compris les données sensibles[67], nécessitent une sécurité et des garanties supplémentaires. Les informations confidentielles, en particulier le secret des affaires, ou les données liées à la sécurité des services des plateformes méritent également une protection appropriée. Parallèlement, le cadre pour l'accès aux données devrait au moins permettre aux chercheurs universitaires d'accéder aux ensembles de données nécessaires pour comprendre les sources, les vecteurs, les méthodes et les modèles de propagation qui caractérisent le phénomène de la désinformation.

À cette fin, le code devrait mettre en place une procédure transparente incluant toutes les parties prenantes concernées, en particulier, les plateformes et la communauté des chercheurs, afin de définir les conditions qui s'appliquent à l'accès à ces ensembles de données. En principe, ces conditions devraient être normalisées et uniformes entre les plateformes. La procédure devrait régir, entre autres, i) les normes et les qualifications minimales des chercheurs auxquels l'accès sera accordé, ii) les catégories minimales de données qui seront mises à disposition, iii) les mesures de sécurité techniques et organisationnelles à respecter concernant le traitement de ces données, y compris la limitation de la finalité et la minimisation des données, et iv) en ce qui concerne les données pseudonymisées, toute mesure nécessaire visant à empêcher qu'elles ne soient réattribuées à une personne donnée[68].

[67] Au sens de l'article 9 du RGPD.

[68] Comme l'exige le RGPD, la divulgation des données à caractère personnel doit être fondée sur une base juridique claire avec des garanties appropriées, notamment les dispositions de l'article 9 pour les catégories spéciales de données.

8.1.4 Rôle de l'EDMO

Compte tenu de son indépendance et de ses fonctions de coordination, l'EDMO pourrait apporter son soutien dans le domaine de l'accès aux données, notamment en fournissant des orientations, entre autres, sur les catégories de données devant être accessibles, les finalités du traitement des données et les mesures de sécurité appropriées relatives au traitement des données à caractère personnel et celles visant à empêcher que les données anonymisées ne soient réattribuées à une personne donnée.

Facilités par l'EDMO, des travaux sont en cours en vue d'étudier les possibilités d'un code de conduite au titre de l'article 40 du RGPD visant à garantir la bonne application des exigences relatives à la vie privée et à la protection des données au partage, par les plateformes, des données à caractère personnel avec les chercheurs. Le RGPD prévoit des conditions générales de traitement des données à caractère personnel aussi sous la forme d'un partage, par les plateformes, de telles données avec les chercheurs. Un tel code réduirait les incertitudes juridiques et les risques pour les plateformes qui accordent un accès à leurs données et garantirait un environnement sécurisé et harmonisé pour le traitement des données à caractère personnel à des fins de recherche[69]. Le code renforcé devrait engager les signataires à faciliter, si nécessaire, l'élaboration du code de conduite prévu à l'article 40 du RGPD.

8.1.5 Accès aux données par les autres parties prenantes

D'autres parties prenantes, telles que les organisations de la société civile, les centres de recherche non universitaires et les journalistes d'investigation, jouent également un rôle important pour déceler et analyser les campagnes de désinformation, formuler des réponses politiques et promouvoir la sensibilisation de la population et la résilience de la société. Les signataires du code devraient permettre, en particulier dans les États membres où les capacités universitaires font défaut, un niveau d'accès suffisant à ces parties prenantes, dans le respect des exigences relatives à la vie privée et sous réserve d'un contrôle renforcé contre les utilisations abusives des données à caractère personnel et la réattribution des données pseudonymisées à une personne donnée.

8.2 Cadre de coopération entre les signataires et les chercheurs

Afin de favoriser une plus grande communauté pluridisciplinaire de chercheurs indépendants et de leur donner les moyens d'agir, le code devrait établir un cadre de coopération transparent, ouvert et non discriminatoire entre les signataires et la communauté des chercheurs de l'UE concernant les ressources et le soutien mis à la disposition des chercheurs. Ce cadre devrait permettre à la communauté des chercheurs de gérer de manière indépendante les fonds que les signataires mettent à leur disposition pour la recherche sur la désinformation, en définissant des priorités scientifiques et des procédures d'attribution transparentes fondées sur le mérite scientifique. À cet égard, l'EDMO pourrait contribuer à l'attribution de ces ressources.

[69] La discussion avec les parties prenantes a permis de mettre en lumière le soutien des signataires du code et de la communauté des chercheurs envers cette initiative: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation.

8.3 Collaboration avec les vérificateurs de faits

Les vérificateurs de faits sont des acteurs importants de la lutte contre le phénomène de la désinformation[70]. Ils évaluent et vérifient les contenus en se fondant sur des faits, des données probantes et des informations contextuelles et sensibilisent les utilisateurs à la désinformation en ligne. Le code renforcé devrait prévoir de soutenir davantage leur travail et d'augmenter la couverture des activités de vérification des faits au sein des États membres et dans les langues de l'UE.

8.3.1 Modes de coopération

Compte tenu des lacunes importantes que présentent les activités de vérification des faits et de la manière inégale dont ces activités sont mises en œuvre selon les services et les États membres[71], les signataires des plateformes devraient s'engager à prendre des mesures concrètes, assorties d'objectifs et d'un calendrier précis, afin de développer leur coopération avec les vérificateurs de faits de manière à garantir la mise en pratique cohérente de la vérification des faits dans leurs services. Les efforts devraient porter en particulier sur les États membres et les langues dans lesquels la vérification des faits n'est pas encore assurée[72].

Pour y parvenir, il serait possible d'envisager des accords multilatéraux entre les plateformes et des organismes indépendants de vérification des faits qui répondent à des normes éthiques et professionnelles élevées. Ces accords devraient être fondés sur des conditions transparentes, ouvertes et non discriminatoires et garantir l'indépendance des vérificateurs de faits. Ils devraient prévoir une rémunération équitable des vérificateurs de faits pour les travaux utilisés par les plateformes, favoriser la coopération transfrontière entre les vérificateurs de faits et faciliter le flux de vérification des faits entre les services des signataires.

Compte tenu de son rôle en matière de promotion des activités conjointes de vérification des faits, l'EDMO est bien placé pour aider les plateformes et les vérificateurs de faits à élaborer un cadre de collaboration, notamment la création d'une interface commune pour les vérificateurs de faits, l'échange d'informations entre ces derniers et la promotion de la coopération transfrontière.[73]

---

[70]Les organismes de vérification des faits publient régulièrement des rapports non partisans sur l'exactitude des déclarations faites par des personnalités publiques et des grandes institutions, ainsi que d'autres affirmations largement diffusées qui présentent un intérêt pour la société. Elles sont indépendantes et suivent des règles d'éthique et de transparence strictes, telles que celles définies par l'International Fact-Checking Network (IFCN ou réseau international de vérification des faits) (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]Carte des activités de vérification des faits dans l'UE de l'EDMO: https://edmo.eu/fact-checking-activities/

[73]Afin de soutenir davantage le travail des vérificateurs de faits européens, leur coopération et l'élaboration de normes professionnelles communes, le projet pilote «Integrity of social media» (Intégrité des réseaux sociaux) soutiendra la rédaction d'un code d'intégrité professionnelle pour les vérificateurs de faits européens, en coopération avec l'EDMO. Voir: programme de travail annuel, adopté au titre de la décision C (2020) 2259 de la Commission.

8.3.2 Utilisation et intégration de la vérification des faits dans les services des signataires

Le code renforcé devrait comporter des engagements exigeant une utilisation et une intégration plus cohérentes du travail des vérificateurs de faits dans les services des plateformes, y compris pour les systèmes de publicité programmatique et les contenus vidéo. Les plateformes devraient s'engager à utiliser des mécanismes permettant d'intégrer la vérification des faits de manière rapide et cohérente dans leurs services après notification par les vérificateurs de faits, y compris un marquage rapide et efficace. Les signataires concernés devraient faciliter la création d'un référentiel commun d'articles de vérification des faits produits par les vérificateurs et étudier des solutions technologiques visant à en faciliter l'utilisation efficace sur toutes les plateformes et dans toutes les langues afin d'empêcher la résurgence d'éléments de désinformation que les vérificateurs de faits ont démentis[74].

8.3.3 Accès des vérificateurs de faits aux informations pertinentes

Afin de maximiser la qualité et l'incidence de la vérification des faits, le code renforcé devrait garantir que les signataires de la plateforme s'engagent à fournir aux vérificateurs de faits un accès automatisé aux informations sur les mesures qu'ils ont prises concernant le contenu reposant sur des faits avérés et les vérifications des faits. Ces informations devraient quantifier i) les interactions des utilisateurs dans le temps (par exemple, le nombre de vues, de mentions «J'aime», de partages, de commentaires avant et après la vérification des faits)[75] avec le contenu reposant sur des faits avérés, et ii) la portée de la vérification des faits dans le temps, sur les services en ligne où elles ont été publiées. Les plateformes et les vérificateurs de faits devraient convenir d'une interface commune pour la vérification des faits afin de garantir la cohérence concernant la manière dont les plateformes utilisent, créditent et commentent le travail des vérificateurs de faits. En outre, le code devrait prévoir un échange régulier d'informations entre ses signataires et la communauté des vérificateurs de faits afin de renforcer la coopération.

9 SUIVI DU CODE

Le code renforcé devrait être complété par un système de suivi solide qui tire parti de l'expérience que la Commission a acquise jusqu'à présent en matière de suivi du code, notamment le programme relatif à la COVID-19. L'amélioration du système de suivi devrait permettre d'évaluer régulièrement la mise en œuvre des engagements du code par les signataires, de favoriser l'amélioration de leurs politiques et actions et d'évaluer l'efficacité du code en tant qu'outil de lutte contre la désinformation. L'amélioration du système de suivi devrait renforcer l'obligation de rendre compte des plateformes en ligne pendant la période transitoire avant l'adoption de la législation sur les services numériques et fournir un cadre permettant, entre autres, un dialogue structuré avec les très grandes plateformes concernant l'élaboration et le déploiement de mesures d'évaluation et d'atténuation des risques, en prévision des obligations juridiques prévues à cet effet dans la proposition relative à la législation sur les services numériques.

[74] En ce qui concerne la création d'un référentiel de vérification des faits, les signataires pourraient rechercher des synergies avec l'EDMO.

[75] Cela devrait aussi inclure les données démographiques anonymisées et l'emplacement des personnes partageant/recevant le contenu reposant sur des faits avérés.

Compte tenu de ces objectifs, les engagements actuels du code en matière de suivi devraient être renforcés et étendus afin de créer un cadre solide qui intègre les éléments fondamentaux exposés ci-après. Le code renforcé devrait notamment garantir que les signataires fournissent en temps utile les informations et les données nécessaires au suivi, dans des formats normalisés et en les ventilant par État membre.

9.1 Indicateurs clés de performance

Le suivi du code devrait reposer sur des ICP capables de mesurer la mise en œuvre et l'efficacité des engagements du code ainsi que l'incidence du code sur le phénomène de la désinformation. À cette fin, deux catégories d'ICP sont pertinentes: i) les indicateurs du niveau de service qui mesurent les résultats et l'incidence des politiques mises en œuvre par les signataires pour remplir leurs engagements au titre du code, et ii) les indicateurs structurels qui mesurent l'incidence globale du code sur la désinformation au sein de l'Union.

9.1.1 Indicateurs du niveau de service

Dans le cadre du code révisé, les signataires devraient s'engager à élaborer des indicateurs concrets du niveau de service. Les indicateurs du niveau de service devraient mesurer efficacement la mise en œuvre des engagements du code et l'incidence des politiques des signataires. Les indicateurs devraient être suffisamment souples pour s'adapter aux différents services des signataires tout en permettant de produire des rapports et des comparaisons cohérents sur les services.

Le code renforcé devrait exiger que les signataires définissent une série minimale d'indicateurs qualitatifs et quantitatifs, en rendent compte et s'engagent à les respecter, afin d'évaluer, entre autres, les points suivants:

- L'incidence des outils et des fonctionnalités mis en place pour renforcer la sensibilisation et la responsabilisation des utilisateurs, y compris les interactions des utilisateurs avec ces outils et fonctionnalités[76].
- L'incidence des outils et des fonctionnalités qui affichent ou rendent plus visibles des informations fiables présentant un intérêt pour le public, y compris les interactions des utilisateurs avec ces outils et fonctionnalités[77].
- Le nombre de vérifications des faits, le pourcentage de contenus vérifiés par rapport aux contenus signalés par les utilisateurs et le financement des activités de vérification des faits.
- L'incidence des activités de vérification des faits et les interactions des utilisateurs avec les informations dont une vérification des faits a révélé le caractère faux ou trompeur[78].

[76]Cette incidence pourrait être mesurée par des indicateurs quantifiant le degré d'interaction (par exemple, les vues, les taux de clics, les partages, etc.) des utilisateurs avec ces outils et qualifiant la perception des utilisateurs en ce qui concerne l'utilité de ces outils. Les indicateurs devraient aussi inclure des données relatives à l'utilisation d'outils permettant de signaler les contenus perçus comme étant faux.

[77]Cette incidence pourrait être mesurée par des indicateurs quantifiant le degré d'interaction (par exemple, le nombre de vues, les impressions, les taux de clics, les partages, etc.) des utilisateurs avec ces outils et qualifiant la perception des utilisateurs en ce qui concerne l'utilité de ces outils.

[78]L'incidence peut être mesurée par des indicateurs quantifiant le degré d'interaction (par exemple, les vues, les taux de clics, les partages) avec des éléments de contenu avant et après qu'ils aient été marqués

- Le nombre de recours liés aux mesures que prennent les plateformes concernant les contenus à la suite du signalement de l'élément de désinformation et les informations relatives à leur issue.
- Le nombre de pages, de comptes, de profils et de groupes partageant des éléments de désinformation qui font l'objet de mesures visant à en réduire la visibilité[79], ainsi que la quantité de contenus partagés.
- L'incidence des comportements manipulateurs interdits qui ont été recensés, notamment les cas de suppression ou de rétrogradation de contenus ou de comptes[80].
- Le nombre de partenariats entre les signataires du code issus du secteur de la publicité et des entités tierces évaluant la qualité des sources d'information.
- L'incidence des mesures employées pour le contrôle des placements de publicité[81].
- La quantité et le niveau de détail des données mises à disposition à des fins de recherche et le nombre d'organismes de recherche européens ayant accès aux données des plateformes.
- La quantité de ressources que les signataires mettent à disposition pour la recherche sur la désinformation et le nombre d'organismes de recherche européens ayant accès à ces ressources.
- Des informations concernant les membres du personnel qui participent au respect des engagements du code[82].

9.1.2 Indicateurs structurels

Les signataires du code devraient également s'engager à contribuer à l'élaboration d'indicateurs structurels permettant de mesurer efficacement l'incidence globale du code sur le phénomène de la désinformation. Tel que décrit ci-après, les signataires devraient mettre en place un groupe de travail permanent chargé notamment d'élaborer, de tester et d'ajuster les indicateurs structurels.

Les indicateurs structurels pourraient, par exemple, se fonder sur des échantillons représentatifs d'utilisateurs dans divers États membres, afin d'évaluer la prévalence des vecteurs constants de désinformation[83] dans les médias en ligne que consomment les citoyens européens[84]. Ces indicateurs pourraient mesurer l'engagement du public vis-à-

---

ou rétrogradés car ils étaient faux. D'autres indicateurs pourraient également renseigner sur la manière dont interviennent les interactions des utilisateurs.

[79]Y compris des mesures telles que la rétrogradation des contenus et la suppression de profils et de groupes.

[80]L'incidence pourrait être mesurée par des indicateurs quantifiant le degré d'interaction (par exemple, les vues, les taux de clics, les partages, etc.) avec le contenu, les comptes et les cas de suppression ou de rétrogradation avant leur suppression et avant et après leur rétrogradation.

[81]L'incidence pourrait être mesurée par des indicateurs quantifiant le nombre de placements publicitaires affichés sur des sites web recensés comme diffusant des éléments de désinformation de manière constante, ainsi que le nombre de publicités contenant des éléments de désinformation qui ont été supprimées.

[82]Cela inclut le nombre de personnes employées pour mener les activités de lutte contre la désinformation et les langues que couvrent leurs activités.

[83]L'identification des vecteurs de désinformation en ligne devrait reposer sur une méthode claire et approuvée, définie par un ensemble plus large de parties prenantes, notamment des chercheurs universitaires, des vérificateurs de faits, des ONG et des organisations de la société civile.

[84]Le mécanisme de mesure des indicateurs structurels pourrait s'inspirer des pratiques mises en œuvre par le secteur audiovisuel pour mesurer les audiences.

vis des sources d'information, ainsi que des enquêtes régulières et normalisées visant à mesurer l'exposition des citoyens à la désinformation.

En attendant qu'une série plus stable d'indicateurs structurels soit mise au point, les signataires et les parties prenantes devraient convenir d'une série minimale viable d'indicateurs structurels qui peuvent être rapidement mis en œuvre et testés, en travaillant à la création d'une série stable d'indicateurs structurels efficaces.

9.2 Cadre de suivi

Le cadre de suivi devrait permettre d'évaluer régulièrement la mise en œuvre des engagements du code par les signataires, y compris les modifications et les évolutions relatives aux politiques et aux actions pertinentes. À cette fin, les signataires devraient rendre compte régulièrement à la Commission de la mise en œuvre de leurs engagements, notamment au moyen des ICP pertinents.

À la suite de l'expérience positive des programmes de suivi lors des élections européennes de 2019[85] et de la pandémie de COVID-19, la Commission s'appuiera sur le soutien du groupe des régulateurs européens pour les services de médias audiovisuels (ERGA) pour suivre la mise en œuvre du code au niveau des États membres. L'EDMO et ses pôles devraient également aider la Commission à analyser les informations et les données communiquées par les signataires et à évaluer l'incidence du code au niveau national et européen.

En tenant compte des conseils d'experts et du soutien de l'ERGA et de l'EDMO, la Commission évaluera régulièrement les progrès réalisés concernant la mise en œuvre du code, ainsi que l'incidence du code sur le phénomène de la désinformation, et publiera ses conclusions. La Commission pourra également fournir de nouvelles orientations sur la manière dont les signataires devraient remédier aux lacunes et aux insuffisances qui subsistent dans le code.

9.2.1 Communication régulière d'informations

Les obligations prévues dans le code renforcé en matière de communication d'informations devraient tenir compte de la taille des signataires et du type de services qu'ils fournissent. Les prestataires de services en ligne dont les services sont utilisés à grande échelle au niveau de l'Union et qui présentent des profils de risque plus élevés en ce qui concerne la diffusion d'éléments de désinformation devraient rendre compte tous les six mois de la mise en œuvre des engagements auxquels ils ont souscrit et fournir des indicateurs correspondants du niveau de service. Ils devraient également évaluer chaque année les risques liés au phénomène de la désinformation. Les autres signataires du code devraient communiquer des informations tous les ans et fournir les données relatives à leurs activités. Les signataires qui fournissent des outils, des instruments ou des solutions visant à lutter contre la désinformation, ou qui soutiennent le code en fournissant leur expertise, devraient également communiquer chaque année des données sur leurs activités et leurs conclusions concernant la mise en œuvre et l'efficacité du code. Les informations devraient être communiquées conformément à un calendrier défini qui fixe les périodes de couverture et les dates limites de présentation. Les données utilisées pour mesurer les ICP devraient être ventilées au niveau des États membres.

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

Les informations communiquées devraient reposer sur un modèle harmonisé permettant, dans la mesure du possible, d'effectuer des comparaisons entre les plateformes. En outre, les signataires devraient convenir d'un ensemble de formats normalisés et vérifiables pour la communication des données relatives aux ICP. Ces formats devraient être élaborés conjointement avec les parties prenantes concernées du groupe de travail permanent et devraient respecter les normes et utiliser les méthodes de la communauté des chercheurs et des vérificateurs de faits. À terme, ces formats devraient permettre de mettre à jour de manière continue un tableau de bord public mis à disposition par le centre de transparence, tel qu'indiqué ci-après.

9.2.2 Centre de transparence

Afin de renforcer la transparence et l'obligation de rendre compte concernant la mise en œuvre du code, les signataires devraient s'engager à créer et à maintenir un centre de transparence accessible au public. Les signataires devraient indiquer dans le centre de transparence les politiques spécifiques qu'ils ont adoptées pour mettre en œuvre chaque engagement du code auquel ils ont souscrit et fournir des informations de base sur la manière dont ces politiques sont appliquées, y compris leur couverture géographique et linguistique. Le centre de transparence devrait également intégrer un tableau de bord public affichant les ICP pertinents. Il devrait être conçu, en particulier, pour permettre d'effectuer des comparaisons entre les services concernant les progrès réalisés par les signataires dans le domaine de la mise en œuvre des engagements du code et des incidences mesurables en ce qui concerne la lutte contre la désinformation. Les signataires devraient s'engager à mettre régulièrement à jour le centre de transparence et à communiquer toute modification des politiques pertinentes au plus tard 30 jours après l'annonce ou la mise en œuvre d'une telle modification.

9.2.3 Groupe de travail permanent

Le code renforcé devrait créer un groupe de travail permanent chargé de faire évoluer et d'adapter le code en fonction de l'évolution des technologies, des sociétés, du marché et de la législation. Le groupe de travail devrait inclure les signataires du code et des représentants de l'EDMO et de l'ERGA et pourrait inviter des experts pertinents à l'aider dans ses travaux. Le groupe de travail devrait être présidé par la Commission et comprendre des représentants du Service européen pour l'action extérieure. Conformément à son objectif général consistant à contribuer à l'examen et à l'adaptation du code, le groupe de travail devrait inclure, entre autres, les activités suivantes:

- l'élaboration d'une méthode d'évaluation des risques et d'un système de réaction rapide à utiliser dans des situations particulières, telles que des élections ou des crises;
- l'examen de la qualité et de l'efficacité du modèle de rapport harmonisé, ainsi que des formats et des méthodes de divulgation des données à des fins de suivi;
- l'optimisation de la qualité et de la précision des données à fournir pour mesurer les indicateurs;
- la contribution à l'évaluation de la qualité et de l'efficacité des indicateurs du niveau de service et à leur adaptation pertinente;
- l'élaboration, les tests et l'ajustement des indicateurs structurels et la conception de mécanismes permettant de les mesurer au niveau des États membres;
- la fourniture d'avis d'experts et de données probantes les plus récentes concernant les engagements du code, notamment les nouveaux types de comportements non authentiques.

10 CONCLUSIONS ET ETAPES SUIVANTES

Les présentes orientations définissent les principaux éléments qui sont nécessaires, selon la Commission, pour transformer le code en un instrument plus solide en vue de lutter contre la désinformation et de créer un environnement en ligne plus sûr et plus transparent.

La Commission invite les signataires du code à se réunir en vue de renforcer le code, conformément aux présentes orientations. La Commission invite les signataires à fournir un premier projet de code révisé à l'automne afin de permettre un véritable débat le concernant. Elle invite également les nouveaux signataires potentiels à adhérer au code et à participer à sa révision, notamment les plateformes anciennes et nouvelles, des représentants d'entreprises et d'autres acteurs du secteur de la publicité en ligne, ainsi que d'autres parties prenantes susceptibles d'apporter des ressources ou une expertise concourant au fonctionnement efficace du code.

La désinformation étant un phénomène qui ne connaît pas de frontières et afin de renforcer l'incidence réelle du code de bonnes pratiques, il serait utile de mener des actions dans le voisinage européen, notamment la collaboration avec la société civile, la coopération avec des professionnels des médias et les initiatives en matière d'éducation aux médias.