



**Conserver ce qui fonctionne,
corriger ce qui ne fonctionne pas :**

Les principes de politique de la FFÉ pour la
législation sur les services numériques

Publié en 2020

Une publication de la Fondation Frontière Électronique (Electronic Frontier Foundation), 2020. « Conserver ce qui fonctionne, corriger ce qui ne fonctionne pas : Les principes de politique de la FFÉ pour la législation sur les services numériques » est diffusée sous licence Creative Commons Attribution 4.0 International (CC BY 4.0).

Contact

Christoph Schmon, directeur des politiques internationales : christoph@eff.org

Demandes des médias : press@eff.org

Registre de transparence de l'UE

805637038375-01

Tables des matières

Conserver ce qui fonctionne, corriger ce qui ne fonctionne pas	4
Conserver ce qui fonctionne : une responsabilité limitée et aucune surveillance.....	6
Obligations d'interopérabilité : donner le contrôle aux utilisateurs et aux innovateurs.....	9
Donner priorité aux utilisateurs : mettre en œuvre des moyens de contrôle renforcés à la disposition des utilisateurs	12
Transparence et justice procédurale : corriger ce qui ne fonctionne pas	15

Conserver ce qui fonctionne, corriger ce qui ne fonctionne pas

Internet a connu des jours meilleurs. Il fut la promesse d'une libération : quiconque dispose d'un appareil informatique peut se connecter au monde, anonymement ou non, pour raconter son histoire, organiser, éduquer et apprendre. Mais aujourd'hui, pour de nombreux utilisateurs, l'expérience en ligne implique d'être limités à quelques puissantes plateformes, d'être suivis à la trace sur la toile sans avoir donné son consentement, avec notre possibilité d'accéder à de l'information et de la partager laissée à la merci de systèmes algorithmiques de décision qui éditent nos vies sur Internet. Les principes fondamentaux tels que la transparence, l'ouverture et l'autodétermination informationnelle qui furent les piliers des débuts d'Internet ont grandement souffert.

Ce n'était pas inévitable et ne doit pas nécessairement être permanent. Nous pouvons façonner Internet, et il dépendra en partie d'une révision minutieuse du droit des technologies dans l'optique de l'économie des plateformes qui caractérise le 21^e siècle. Nous pouvons améliorer ce qui existe, mais nous devons protéger les éléments de l'ordre juridique actuel qui fonctionnent.

Dans l'Union européenne, il existe précisément une occasion de le faire : adopter une législation pérenne qui conserve les règles qui ont inspiré l'innovation et protégé les droits fondamentaux, tout en donnant le contrôle aux utilisateurs et aux innovateurs futurs. En 2020, la Commission européenne a annoncé une [stratégie](#) ambitieuse pour promouvoir une vision clairement européenne de réglementation des géants de la technologie. La législation sur les services numériques représente une partie de cette stratégie. La [législation sur les services numériques](#) (LSN) est la plus importante réforme de la réglementation européenne des plateformes, la [directive sur le commerce électronique](#), que l'UE a entreprise en vingt ans. C'est une occasion unique de formuler une vision audacieuse et fondée sur des données factuelles afin de répondre aux défis les plus urgents de notre temps.

Nous appuyons l'engagement de la Commission en faveur d'un avenir différent et meilleur pour Internet, et nous saluons son ambition de trouver des solutions novatrices à des problèmes complexes, tels que les échecs en matière de transparence, la modération privatisée des contenus, ainsi que les marchés dominés par les contrôleurs d'accès. Nous avons déjà [contribué](#) aux rapports du Parlement européen et à la consultation de la Commission sur la LSN, et nous continuerons de travailler en étroite collaboration avec les institutions de l'UE afin de partager nos expériences de lutte pour les droits numériques par des procès sur les répercussions, l'activisme sur le terrain et le développement des technologies.

Mais nous restons aussi sur nos gardes. Des lois récentes telles que la [directive sur le droit d'auteur](#) et des initiatives réglementaires en [Allemagne](#), en [France](#) et en [Autriche](#), qui tentent de répondre à des problèmes semblables, ont compromis la liberté d'expression sur Internet tout en donnant aux plateformes privées des responsabilités encore plus grandes de contrôle du contenu des utilisateurs. La LSN est une occasion importante de clarifier l'engagement de l'EU envers les droits fondamentaux sur Internet et de négocier des droits de base qui serviront de fondation pour les années à venir.

Dans notre défense des politiques qui entourent la LSN, nous nous concentrerons sur quatre domaines clés : la responsabilité des plateformes, les mandats d'interopérabilité, la justice procédurale et le contrôle par les utilisateurs. Alors que nous avons présenté les principes qui guideront notre travail en matière de politiques, notre message à l'UE a été clair : conservez ce qui fonctionne, corrigez ce qui ne fonctionne pas. Et redonnez le contrôle aux utilisateurs.



Une responsabilité limitée et aucune surveillance : conserver ce qui fonctionne

Principe 1 : Les intermédiaires en ligne ne devraient pas être tenus responsables du contenu des utilisateurs

Les intermédiaires ont un rôle essentiel à jouer afin de garantir la disponibilité des contenus et le développement d'Internet. Ils sont un moteur de la liberté d'expression, car ils permettent aux gens de partager des contenus avec leur public sur une échelle sans précédent. Une des raisons du succès des intermédiaires en ligne est l'immunité dont ils profitent pour le contenu tiers.

C'est l'un des principes fondamentaux qui doit, d'après nous, continuer à étayer la réglementation d'Internet : les plateformes ne devraient pas être tenues responsables des idées, des images, des vidéos ou des propos que les utilisateurs publient ou partagent en ligne. Si un tel principe ne prévalait pas, les plateformes seraient poussées à surveiller expressément le comportement des utilisateurs; elles filtreraient et vérifieraient le contenu des utilisateurs; elles bloqueraient et supprimeraient tout ce qui est controversé, offensant et potentiellement illicite afin d'éviter une responsabilité juridique. Dans le même esprit, les utilisateurs ne seraient en premier lieu certainement pas enclins à s'exprimer librement; ils éviteraient de partager leur expression artistique ou de publier quelque essai critique sur les évolutions d'ordre politique. Pire encore, sans protection juridique, les fournisseurs de services pourraient facilement devenir les cibles d'entreprises, de gouvernements ou de gens mal intentionnés qui souhaitent cibler leurs utilisateurs et les réduire au silence.

L'UE devrait par conséquent faire en sorte que les intermédiaires en ligne continuent de profiter d'exonérations complètes de responsabilité et qu'ils ne soient pas tenus responsables du contenu provenant des utilisateurs. La distinction actuelle nébuleuse entre les fournisseurs d'hébergement passifs ou actifs, pour que les exonérations s'appliquent, devrait être abandonnée : les intermédiaires ne devraient pas être tenus responsables du contenu des utilisateurs tant qu'ils ne sont pas impliqués à la co-création ou à la modification de ce contenu d'une façon qui pourrait substantiellement contribuer à son illégalité, et à condition qu'ils ne connaissent effectivement pas le caractère illicite de ce contenu. Toute obligation supplémentaire doit être proportionnelle et ne doit être un obstacle ni à la liberté d'expression des utilisateurs ni à l'innovation.

Principe 2 : seules les ordonnances des tribunaux devraient déclencher la responsabilité

Les intermédiaires ne devraient pas être tenus responsables s'ils décident de ne pas retirer un contenu simplement parce qu'ils ont reçu le signalement privé d'un utilisateur. Afin de protéger la liberté d'expression, l'UE devrait adopter comme principe que les intermédiaires ne prennent effectivement connaissance d'une illégalité que si cette dernière leur est signifiée par l'ordonnance d'un tribunal. Des entités judiciaires indépendantes devraient seules décider de la légalité du contenu d'un autre utilisateur, pas les plateformes ni les utilisateurs mécontents. Toute exception à ce principe devrait se limiter à du contenu qui est manifestement illicite, c'est-à-dire du contenu qui est illicite de manière évidente, quel que soit le contexte. Les avis concernant un tel contenu devraient être suffisamment précis et documentés.

Principe 3 : Aucune surveillance ni aucun filtrage obligatoire

Dans le cadre la directive actuelle sur le commerce électronique, l'interdiction de la surveillance généralisée a pour objectif de protéger les utilisateurs en garantissant leur liberté d'expression et leurs droits aux données personnelles enchâssés dans la Charte des droits fondamentaux. Si ce principe important devait être abandonné, cela aurait non seulement des conséquences désastreuses sur la liberté des utilisateurs, mais cela mènerait aussi inévitablement à une régulation fantôme, c'est-à-dire une exécution privatisée de ces règlements par des plateformes sans transparence, ni obligation de rendre des comptes ni autres dispositifs de protection.

Il ne devrait par conséquent pas être permis aux États membres de l'Union européenne d'imposer aux fournisseurs de services numériques de surveiller expressément la présence de contenus illicites publiés, transmis ou stockés par les utilisateurs sur leurs plateformes ou réseaux. Les plateformes ne devraient pas non plus avoir l'obligation générale de surveiller activement les faits ni les circonstances qui indiqueraient l'activité illicite d'utilisateurs. L'interdiction des obligations de surveillance généralisée devrait aussi comprendre l'interdiction des systèmes automatisés de filtrage imposé qui évaluent la légalité de contenus tiers ou qui préviennent le (re)téléversement d'un contenu illicite. De plus, aucune responsabilité ne devrait être fondée sur l'incapacité d'un intermédiaire à détecter un contenu illicite. Les droits à la vie privée connexes, tels que le [droit de ne pas être sujet à une prise de décision individuelle automatisée](#), doivent aussi être protégés dans ce contexte.

Principe 4 : Limiter la portée des ordonnances de retrait

Des cas récents ont démontré les dangers des ordonnances à portée mondiale de retrait d'un contenu. Dans le cas [Glawischnig-Piesczek](#), la Cour de justice de l'UE a jugé que le tribunal d'un État membre peut ordonner aux plateformes non seulement de retirer à l'échelle mondiale un contenu diffamatoire, mais aussi de retirer des contenus identiques ou « équivalents ». Cette issue était terrible, car le contenu en question

Les principes de politique de la FFÉ pour la législation sur les services numériques pourrait être considéré comme illicite dans un État, mais totalement licite dans de nombreux autres États. De plus, en faisant référence à des « technologies automatisées » pour détecter des propos semblables, la Cour a ouvert les portes de la surveillance par des filtres, filtres qui sont notoirement inexacts et susceptibles de bloquer à l'excès des contenus légitimes.

La réforme de la législation relative à Internet de l'UE est une occasion de reconnaître qu'Internet est mondial, et que des ordonnances de retrait dont la portée est mondiale sont extrêmement injustes et portent atteinte à la liberté des utilisateurs. Les nouvelles règles devraient veiller à ce que les ordonnances des tribunaux, et particulièrement les injonctions, ne soient pas utilisées pour superposer les lois d'un pays à celles de tous les États du monde. Les ordonnances de retrait devraient être limitées au contenu en question et fondées sur les principes de nécessité et de proportionnalité pour ce qui est de la portée géographique. Il serait autrement possible que nous voyions le gouvernement d'un pays dicter ce que les résidents d'autres pays peuvent dire, voir et partager sur Internet. Cela entraînerait un « mouvement vers le bas » qui créerait un Internet mondial de plus en plus restrictif.



Obligations d'interopérabilité : donner le contrôle aux utilisateurs et aux innovateurs

Principe 1 : Des obligations générales d'interopérabilité

La vision de la FFÉ est un cadre juridique propice à l'innovation et qui redonne aux utilisateurs le contrôle de leurs données, de leur vie privée et de leurs expériences en ligne. Nous croyons que l'interopérabilité a un rôle essentiel à jouer pour donner vie à cette vision d'un Internet d'intérêt public. C'est pourquoi nous proposons des obligations d'interopérabilité pour les plateformes dont le pouvoir de marché est important. Ce que nous voulons dire par cela est simple : les plateformes qui contrôlent les parts importantes d'un marché et qui agissent en tant que contrôleuses d'accès à ce marché doivent offrir aux nouvelles plateformes concurrentes des possibilités d'interagir avec leurs fonctions clés.

Alors que le RGPD donne déjà aux Européens le droit à la portabilité des données, ce droit n'est pas sans limites. Il n'est pas global (les utilisateurs ne peuvent pas porter toutes les données personnelles), il est conditionnel (seulement si cela est « techniquement possible »), et il est difficile de déterminer vers quoi les utilisateurs devraient porter leurs données. L'interopérabilité est la pièce manquante pour donner vie au droit à la portabilité. Une interopérabilité grâce à des interfaces techniques permettrait aux utilisateurs de communiquer avec leurs amis par-delà les frontières des plateformes, ou de pouvoir suivre leurs contenus favoris sur différentes plateformes sans avoir à créer plusieurs comptes. Les utilisateurs ne seraient plus obligés de rester sur une plateforme qui ne respecte ni leur vie privée ni leurs données personnelles, qui recueille secrètement leurs données ou qui met leur sécurité en danger, de peur de perdre leur réseau social. Les utilisateurs devraient plutôt avoir la possibilité de faire des choix réels et éclairés.

Principe 2 : Le pouvoir de délégation

Mais cela n'est pas tout. Il devrait aussi y avoir interopérabilité au niveau des interfaces utilisateur et elle devrait permettre autant de flexibilité et de diversité que les utilisateurs veulent. Par conséquent, les plateformes dont le pouvoir de marché est important devraient aussi permettre à des tiers d'agir au nom des utilisateurs. Si les utilisateurs le veulent, ils devraient pouvoir déléguer certains éléments de leur expérience en ligne à différents intervenants compétents. Par exemple, si vous n'aimez pas les pratiques de modération du contenu de Facebook, vous devriez pouvoir déléguer cette tâche à un autre organisme, tel qu'un organisme sans but lucratif spécialisé dans une modération du contenu fondée sur la communauté.

Principe 3 : Limiter l'utilisation commerciale des données

Afin d'éviter l'exploitation de cette interopérabilité, aucune donnée rendue disponible par cette interopérabilité ne devrait l'être pour une utilisation commerciale générale. La plupart des plateformes importantes sont construites sur des modèles d'entreprise qui reposent sur la collecte (souvent secrète) et la vente des données des utilisateurs; elles monétisent ainsi l'attention des utilisateurs et exploitent leurs données personnelles. Par conséquent, toutes les données rendues disponibles dans le cadre de cette interopérabilité ne devraient être utilisées que pour maintenir l'interopérabilité, protéger la vie privée des utilisateurs ou garantir la sécurité des données. En interdisant l'utilisation commerciale de données utilisées pour la mise en place ou le fonctionnement de l'interopérabilité, nous voulons encourager positivement les concurrents dont les modèles d'entreprise sont innovants, responsables et qui protègent la vie privée et les données personnelles.

Principe 4 : La vie privée et la confidentialité

Il est essentiel de donner aux utilisateurs le pouvoir de contrôler comment, quand, pourquoi et avec qui leurs données sont partagées. Cela signifie que les principes clés qui sous-tendent le RGPD ainsi que les autres législations applicables, telles que la minimisation des données, la confidentialité dès la conception et la confidentialité par défaut doivent être respectés. Cela devrait aussi comprendre des interfaces faciles à utiliser grâce auxquelles les utilisateurs peuvent donner leur consentement explicite pour toute utilisation de leurs données (et aussi révoquer ce consentement n'importe quand).

Principe 5 : La sécurité

Mais les données et les communications des utilisateurs ne devraient pas seulement rester confidentielles, mais aussi protégées. Les mesures d'interopérabilité devraient toujours être axées sur la sécurité des utilisateurs et ne devraient jamais être interprétées comme une raison qui empêche les plateformes de chercher à assurer la sécurité des utilisateurs. Cependant, si les intermédiaires doivent, par nécessité, interrompre l'interopérabilité pour corriger des problèmes de sécurité, ils ne devraient pas exploiter de telles situations pour rompre l'interopérabilité, mais plutôt communiquer de façon transparente, résoudre le problème et rétablir les interfaces d'interopérabilité dans un délai raisonnable et clairement défini.

Principe 6 : La documentation et la non-discrimination

Enfin, il est essentiel de s'assurer que l'interopérabilité ne devient pas un outil que les puissantes plateformes établies utiliseraient pour contrôler l'accès et consacrer davantage leur position dominante. Plus fortes sont la diversité et la pluralité, mieux notre objectif de donner le contrôle aux utilisateurs est servi. Autant de concurrents que possible devraient donc profiter de l'interopérabilité, au lieu de quelques acteurs favorisés. Pour offrir un plus grand choix aux utilisateurs, l'accès aux interfaces d'interopérabilité ne devrait pas faire de distinction entre les différents concurrents, ni être accompagné d'obligations contraignantes ni de restrictions de contenu. Les interfaces d'interopérabilité telles que les API doivent aussi être faciles à trouver, bien documentées et transparentes.



Donner priorité aux utilisateurs : mettre en œuvre des moyens de contrôle renforcés à la disposition des utilisateurs

Principe 1 : Donner aux utilisateurs le contrôle du contenu

De nombreux services tels que Facebook et Twitter présentaient initialement une liste strictement chronologique de publications d'amis des utilisateurs. Au fil du temps, la plupart des plateformes importantes ont changé cette présentation chronologique pour des algorithmes plus complexes (et opaques) qui trient, éditent et distribuent les contenus en ajoutant publicités et autres contenus promotionnels. Ces algorithmes déterminés par les plateformes ne sont pas nécessairement axés sur la satisfaction des besoins des utilisateurs et ne cherchent habituellement à atteindre qu'un seul but : augmenter au maximum l'attention des internautes et le temps qu'ils passent sur un site Web donné. Les publications qui reçoivent le plus d'« engagement » sont priorisées, même si cet engagement est motivé par des émotions fortes telles que la colère ou le désespoir provoqués par la publication. Bien que les utilisateurs puissent parfois retourner au fil chronologique, la conception de l'interface des plateformes les incite souvent à délaisser ce fil chronologique. Les interfaces qui trompent ou manipulent les utilisateurs, dont les « [interfaces truquées](#) », contreviennent souvent aux principes de base des lois européennes sur la protection des données et devraient être traitées, le cas échéant, dans la législation sur les services numériques.

Les outils algorithmiques des plateformes tirent parti de leur connaissance intime de leurs utilisateurs, un assemblage de milliers de points de données apparemment sans rapport. Nombre des inférences qui résultent de ces données semblent

inattendues pour les utilisateurs : les plateformes ont accès à des données qui vont plus loin dans le temps que la plupart des utilisateurs ne le réalisent, et elles sont à même de tirer des conclusions d'après des comportements à la fois individuels et collectifs. Les hypothèses sur les préférences des utilisateurs sont souvent établies en concluant des inférences à partir de points de données apparemment sans rapport. Cela peut orienter (et souvent limiter) les façons dont les utilisateurs peuvent interagir avec les contenus en ligne, et peut aussi amplifier la mésinformation et la polarisation, de sorte à saper l'échange transparent et délibéré de l'information sur lequel nos sociétés démocratiques sont bâties.

Les utilisateurs n'ont pas à accepter cela. De nombreux greffons tiers transforment l'apparence et le contenu des plateformes sociales selon les besoins et les préférences des utilisateurs. Mais à l'heure actuelle, la plupart de ces greffons demandent des compétences techniques pour les trouver et pour les installer, et les plateformes sont fortement motivées à cacher et à empêcher l'adoption par les utilisateurs de tels outils indépendants. La LSN est pour l'Europe l'occasion en or de créer un environnement juridique plus accueillant afin d'encourager et de soutenir ce marché orienté vers l'utilisateur. Le règlement devrait soutenir [l'interopérabilité et permettre une compatibilité concurrentielle](#), et il devrait aussi établir des règles explicites et applicables contre des conditions générales d'utilisation trop agressives qui tendent à interdire toute ingénierie inverse et interconnexion. Par-delà la législation sur les services numériques, l'UE doit soutenir activement en Europe les projets à code source ouvert et commerciaux qui offrent des systèmes frontaux pour les plateformes, adaptés sur le plan linguistique et culturel ou qui donnent le contrôle aux utilisateurs, et aider à favoriser un marché dynamique et durable pour ces outils.

Donner aux gens plus de contrôle sur le contenu, et non aux plateformes, est une étape essentielle pour traiter certains des problèmes omniprésents en ligne et qui sont actuellement si mal gérés par les pratiques de modération des contenus. Les contrôles utilisateur ne devraient pas exiger un niveau élevé d'alphabétisation électronique pour parcourir le Web en toute sécurité.

L'on devrait plutôt donner aux utilisateurs de plateformes de réseautage social qui occupent un pouvoir de marché important la possibilité de choisir le contenu avec lequel ils veulent interagir, et éliminer par filtrage le contenu qu'ils ne veulent pas voir, d'une manière simple et conviviale. Les utilisateurs devraient aussi avoir l'option de refuser complètement les recommandations éditées algorithmiquement ou de choisir d'autres heuristiques pour organiser les contenus.

Principe 2 : La transparence algorithmique

Outre recevoir un contrôle accru du contenu avec lequel ils interagissent, les utilisateurs méritent aussi plus de transparence de la part des entreprises afin de comprendre pourquoi un contenu ou des résultats de recherche leur sont présentés ou cachés. Les plateformes en ligne devraient fournir des renseignements pertinents sur les outils algorithmiques qu'elles utilisent pour modérer le contenu (c'est-à-dire les systèmes de recommandation de contenu, les outils de signalement du contenu) et pour éditer les contenus (par exemple pour le classement vers le haut ou vers le bas des contenus). Les plateformes devraient aussi offrir des explications facilement accessibles, qui permettraient aux utilisateurs de comprendre quand, pour quelles tâches et à quel point les outils algorithmiques sont utilisés. Pour alléger le fardeau qu'est, pour les utilisateurs, la compréhension de la manière dont les algorithmes

sont utilisés, les plateformes au pouvoir de marché important devraient permettre aux chercheurs indépendants et aux organismes de régulation pertinents de contrôler leurs outils algorithmiques afin de garantir qu'ils sont utilisés comme prévu.

Principe 3 : Une gouvernance qui rend des comptes

Les plateformes en ligne gouvernent leurs utilisateurs grâce à leurs conditions générales d'utilisation, leurs orientations communautaires ou leurs normes. Ces documents impliquent souvent les règles fondamentales qui déterminent ce que les utilisateurs sont autorisés à faire sur une plateforme et quel comportement est restreint. Les plateformes mettent régulièrement ces documents à jour, parfois de façon marginale, mais parfois de façon importante et habituellement sans consulter leurs utilisateurs ni leur signaler les changements. Tout changement aux règles qui gouvernent de telles plateformes doit être signalé aux utilisateurs; leur consentement doit leur être demandé et ils devraient être informés des conséquences de leur choix. Une explication satisfaisante de tout changement substantiel devrait aussi leur être présentée en des termes qu'ils comprennent. De plus, les plateformes devraient présenter leurs conditions générales d'utilisation dans un format lisible par machine et rendre toutes les versions précédentes de leurs conditions générales d'utilisation facilement accessibles au public.

Principe 4 : Le droit à l'anonymat en ligne

Les raisons pour lesquelles des individus pourraient ne pas vouloir partager publiquement leur identité en ligne sont innombrables. Alors que l'anonymat était une chose relativement habituelle sur Internet, rester anonyme en ligne est progressivement devenu plus difficile. Dans leur espoir de s'attaquer aux discours haineux ou aux « fausses nouvelles », les stratèges de l'UE et en dehors de l'UE proposent aux plateformes le devoir d'imposer les noms légaux.

Cependant, pour de nombreuses personnes, dont les membres de la communauté LGBTQ+, les travailleurs et travailleuses de l'industrie du sexe et les victimes de violence familiale, de telles règles pourraient avoir des effets dévastateurs et mener à du harcèlement et à d'autres formes d'attribution. Nous croyons qu'en principe les États membres devraient respecter la volonté des individus de ne pas divulguer leur identité en ligne. La législation sur les services numériques devrait aussi confirmer l'autodétermination informationnelle des utilisateurs et présenter le droit européen à l'anonymat sur Internet. Les conditions générales d'utilisation contrevenantes devraient être sujettes au contrôle de leur équité.



Transparence et justice procédurale : corriger ce qui ne fonctionne pas

Principe 1 : Les mécanismes de signalement

Les intermédiaires [ne devraient pas être tenus responsables de choisir de ne pas retirer un contenu](#) simplement parce qu'ils ont reçu le signalement privé d'un utilisateur. Sauf exception, l'UE devrait adopter pour principe que les intermédiaires ne prennent effectivement connaissance d'une illégalité que si l'ordonnance d'un tribunal leur est présentée.

Cependant, l'UE devrait adopter des règles harmonisées sur les mécanismes de signalement qui aident les utilisateurs à signaler aux plateformes un contenu ou un comportement potentiellement illicite. Le signalement d'un contenu potentiellement illicite sur Internet semble simple, mais représente souvent un défi en pratique.

Différentes plateformes utilisent différents systèmes pour signaler un contenu ou des activités, et les catégories utilisées pour différencier les types de contenus peuvent grandement varier; elles peuvent aussi porter à confusion et être difficiles à comprendre. Certaines plateformes ne proposent aucune option significative de signalement. Il devrait être facile de signaler un contenu potentiellement illicite et les actions de suivi de la plateforme devraient être transparentes aux yeux de ses utilisateurs.

Principe 2 : Une norme pour la transparence et l'équité d'avis et d'action

La modération du contenu est souvent opaque; les entreprises ne communiquent généralement pas aux utilisateurs suffisamment de renseignements pour indiquer quels propos sont permis ou pourquoi certaines parties d'un contenu ont été retirées. Afin de rendre la modération du contenu plus transparente, les plateformes

devraient transmettre aux utilisateurs un avis quand un contenu a été retiré (ou quand leur compte a été désactivé). Un tel avis devrait indiquer le contenu retiré, la règle précise qu'il enfreignait et la façon dont le contenu a été détecté. Elle devrait aussi offrir une explication facilement accessible du processus par lequel l'utilisateur peut appeler de la décision.

Les plateformes devraient offrir un processus d'appel convivial, visible et rapide afin de permettre une résolution tangible des litiges de modération du contenu. Les mécanismes d'appel doivent aussi être accessibles, faciles à utiliser et suivre une chronologie communiquée clairement. Elles devraient permettre aux utilisateurs de présenter des renseignements supplémentaires et doivent comprendre un examen par un être humain. À la fin du processus d'appel, les utilisateurs devraient être contactés et l'on devrait leur fournir une déclaration qui explique le raisonnement qui sous-tend la décision prise, avec une formulation que l'utilisateur peut comprendre. Il est aussi essentiel de communiquer aux utilisateurs que même s'ils participent à un processus de résolution de litige, ils ne renoncent pas à leurs droits de demander justice devant des autorités judiciaires indépendantes, telles qu'un tribunal dans leur pays de résidence.

Principe 3 : Ouvrir la boîte noire que sont les processus décisionnels automatisés

La plupart des plateformes utilisent des algorithmes pour automatiser une partie de leurs pratiques de modération du contenu. La modération du contenu est un travail [précaire](#) et [risqué](#), et nombreux sont ceux qui espèrent que les outils automatisés de modération du contenu pourraient être la solution miracle qui résoudrait les nombreux problèmes qui affectent la modération du contenu. Malheureusement, le processus de modération du contenu est délicat et complexe, il dépend grandement du contexte et il est incroyablement difficile de le mener à bien. De plus, les outils automatisés de modération font de [très, très nombreuses erreurs](#). Ces défis sont devenus particulièrement évidents au cours de la pandémie de COVID-19, alors que de nombreuses plateformes ont remplacé les modérateurs humains par des [outils automatisés de modération du contenu](#).

Compte tenu des défauts fondamentaux inhérents à la modération du contenu, les plateformes devraient être aussi transparentes que possible sur leur utilisation d'outils algorithmiques. Si les plateformes font appel à la prise de décision automatisée pour restreindre le contenu, elles devraient indiquer à quelle étape du processus les outils algorithmiques ont été utilisés, expliquer la logique qui sous-tend les décisions automatisées qui ont été prises, et aussi expliquer comment les utilisateurs peuvent contester les décisions.

Principe 4 : Rétablir les contenus retirés à tort

Les systèmes de modération du contenu font constamment des erreurs qui peuvent causer des préjudices réels, qu'ils soient gérés par des êtres humains ou automatisés. Les efforts de modération de contenus considérés offensants ou licites ont des [impacts disproportionnés sur des groupes déjà marginalisés](#). La modération du contenu interfère souvent avec les [contre-discours](#), les tentatives de [réappropriation](#) de termes particuliers, ou les [appels contre le racisme](#) en partageant les propos racistes tenus.

Les décisions erronées de modération du contenu sont si habituelles et ont des effets si négatifs qu'il est essentiel que les plateformes rétablissent le contenu des utilisateurs si la décision de retrait ne peut pas être justifiée par une interprétation raisonnable des règles des plateformes, ou si le retrait était simplement une erreur. La législation sur les services numériques devrait promouvoir un rétablissement rapide et facile des contenus retirés à tort et des comptes désactivés de manière erronée.

Principe 5 : Une surveillance réglementaire coordonnée et efficace

De bonnes lois sont essentielles, mais leur application est tout aussi importante. Les législateurs européens devraient par conséquent faire en sorte que des autorités indépendantes tiennent les plateformes responsables. La coordination entre les autorités nationales indépendantes devrait être renforcée afin de permettre une application à l'échelle de l'UE, et les plateformes devraient être incitées à respecter leurs devoirs de diligence raisonnable, par exemple par des sanctions harmonisées concrètes dans toute l'Union européenne.