GLOBAL NETWORK INITIATIVE

CONTENT REGULATION AND HUMAN RIGHTS

RÉSUMÉ ANALYTIQUE

NOTRE POINT DE DÉPART

Les principes de bonne gouvernance et les droits de l'homme incitent les gouvernements à comprendre et à aborder les préjudices publics et privés relevant de leur compétence. Comme les décideurs et les régulateurs partout dans le monde affichent une préoccupation croissante au regard des diverses formes de contenus et de comportements en ligne, il n'est pas surprenant que beaucoup réfléchissent aux diverses actions publiques pouvant aider ou entraver les efforts visant à répondre à ces préoccupations.

L'Initiative de réseau global (Global Network Initiative - GNI - dans sa version originale en anglais), une initiative multipartite, a passé en revue plus d'une douzaine d'initiatives gouvernementales récentes[1] qui prétendent aborder diverses formes de préjudice en ligne liées au contenu généré par les utilisateurs, une pratique que nous appelons généralement la « réglementation du contenu ». Nous nous sommes concentrés sur des propositions qui pourraient transférer les responsabilités existantes et les incitations liées au contenu généré par les utilisateurs. Notre analyse illustre la manière dont

1. Ce résumé comprend l'analyse de nombreuses initiatives de réglementation des contenus que les membres de la GNI ont identifiées comme dignes d'intérêt jusqu'à son impression à la mi-septembre 2020.

les principes de bonne gouvernance et les droits de l'homme fournissent une orientation éprouvée permettant de créer et mettre en œuvre de la manière la plus appropriée et la plus efficace possible des lois, des règlements et des mesures stratégiques. Comme la réglementation du contenu est principalement axée sur la communication et les contenus numériques, et est susceptible d'avoir un impact sur ceux-ci, nous nous fondons principalement sur les principes internationaux des droits de l'homme liés à la liberté d'expression et à la vie privée.

Ces principes des droits de l'homme historiquement éprouvés peuvent aider les législateurs à trouver des moyens créatifs et appropriés pour mobiliser les parties prenantes, concevoir des réglementations adaptées aux besoins et atténuer les conséquences inattendues. **Les gouvernements qui placent activement les droits de l'homme au premier plan de leurs délibérations et de leurs développements sont non seulement moins susceptibles de violer leurs propres engagements les plus essentiels, mais ils peuvent également obtenir des résultats plus éclairés et plus efficaces**, équilibrer les responsabilités publiques et privées, concevoir des incitations appropriées, renforcer la confiance et favoriser l'innovation.

NOS CONSTATATIONS

Bien qu'il y ait des différences importantes entre les divers efforts de réglementation du contenu examinés dans le présent résumé, bon nombre d'entre eux partagent certaines caractéristiques principales. Par définition, de telles initiatives modifient l'équilibre des responsabilités dans l'écosystème des technologies de l'information et des communications (TIC), en introduisant un degré **d'incertitude juridique**. Cela peut modifier la compréhension et les attentes des utilisateurs, perturber les chaînes de valeur informationnelles et risquer de perturber les règles du jeu pour les entreprises des TIC indépendamment de leur taille et de leur modèle commercial. Bien que ce ne soit pas, en soi, une raison pour s'abstenir de réglementer, peu de gouvernements ont fait preuve d'efforts suffisants pour bien comprendre les répercussions sociales et économiques de telles perturbations.

De nombreux efforts de régulation du contenu **nécessitent ou incitent fortement les intermédiaires à s'appuyer davantage sur les systèmes de filtrage automatiques** pour identifier de manière proactive les contenus ou comportements illégaux ou inappropriés, même si ces systèmes, dans leur état actuel, peuvent entraîner une suppression excessive et augmenter le risque d'autocensure.[2] Au-delà de cet aspect, un certain nombre des initiatives étudiées **obligeraient les intermédiaires à statuer rapidement sur la légalité ou la recevabilité du contenu tiers sur leurs services**, ce qui aurait des conséquences imprévues et complexes pour la primauté du droit, le processus démocratique, la responsabilisation et les recours.

2. *Voir* l'article de Natasha Duarte et Emma Llansó, « Mixed message? The Limits of Automated Social Media Content Analysis »(disponible en anglais uniquement) du 28 novembre 2017 à l'adresse https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/.

De plus, certaines de ces initiatives **nécessitent implicitement ou explicitement le suivi et/ou l'attribution de contenu, ce qui soulève des préoccupations importantes relatives à la confidentialité**. Les législateurs ont été particulièrement mis à au défi dans leurs efforts pour réglementer les services de messagerie privée, dont beaucoup sont dotés d'un chiffrement de bout en bout fort, qui protège le contenu et la sécurité des utilisateurs, mais peut rendre difficile la modération de contenu par des intermédiaires.

Enfin, un certain nombre de ces efforts **s'appliquent plus largement que nécessaire**. Certains cherchent non seulement à lutter plus efficacement contre l'expression illégale, mais aussi à réglementer les contenus licites, mais nuisibles. D'autres, que ce soit explicitement ou en raison d'un langage peu clair, s'appliquent à des entreprises de tailles diverses dans les différentes couches du secteur des TIC, créant inutilement un potentiel de responsabilité parmi les entreprises qui ne sont pas bien placées pour traiter efficacement ou proportionnellement les contenus. D'autres encore affirment leur autorité à réglementer le contenu de manière extraterritoriale, voire mondiale, sans tenir compte des implications pour les droits des utilisateurs dans d'autres juridictions et de la courtoisie internationale.

NOS RECOMMANDATIONS[3]

Afin d'identifier des approches efficaces et proportionnées à la réglementation du contenu, les autorités **publiques doivent reconnaître que le secteur des TIC est en constante évolution**. Les services qui facilitent le partage de contenu généré par les utilisateurs diffèrent de manière importante et le secteur des TIC présente un écosystème d'éléments interdépendants sur lequel reposent de nombreuses industries, initiatives et possibilités. Cette complexité appelle un examen minutieux des mesures les plus appropriées et les plus étroitement adaptées aux défis spécifiques à relever. Les législateurs doivent être clairs sur les priorités qui guident leurs efforts et ouverts à diverses approches pour les atteindre.

Heureusement, de nombreux acteurs sont d'accord sur la nécessité de répondre aux préoccupations légitimes de politique publique concernant les contenus et les comportements préjudiciables en ligne dans le respect des droits de l'homme. De nombreuses entreprises de TIC ont fini par reconnaître la valeur de lois et d'obligations claires et définies publiquement, tandis que les acteurs de la société civile continuent de fournir des conseils constructifs et souvent prémonitoires tirés des expériences réelles des communautés les plus vulnérables et marginalisées. **Les processus de délibération législative doivent donc être ouverts et non contradictoires, en s'appuyant sur une vaste expertise** pour s'assurer que les résultats sont bien pensés et fondés sur des preuves. Les organes de régulation ou de surveillance non élus devraient également donner la priorité à la transparence et à la consultation avec les différents groupes.

De plus, même si les gouvernements peuvent et doivent apprendre les uns des autres, ils doivent également reconnaître **qu'il n'existe pas de solutions prêtes à l'emploi pour relever des défis réglementaires complexes**. Les gouvernements doivent

3. Remarque : une série complète de recommandations se trouve à l'annexe A à la fin du présent document.

prendre le temps de comprendre et d'envisager des mesures conformes aux obligations internationales relatives aux droits de l'homme, appropriées et proportionnées à leur juridiction.

Bien qu'il soit clair que les entreprises des TIC ont des responsabilités et des rôles importants à jouer dans la lutte contre les préjudices en ligne, **les législateurs devraient résister à la tentation de transférer toute responsabilité légale de ceux qui génèrent du contenu illégal à des intermédiaires**. Cela peut faire dévier les priorités de l'entreprise, en incitant à une surveillance envahissante et à la suppression excessive de contenu, tout en ne permettant souvent pas en parallèle de s'attaquer aux facteurs sous-jacents des contenus et comportements nuisibles.

Les lois et règlements régissant le secteur des TIC devraient également être étroitement ciblés et encadrés. Les législateurs devraient prêter une attention particulière à la façon dont les lois et les règlements auront un impact sur les entreprises ayant des modèles d'affaires différents, en cherchant à **favoriser une diversité de services numériques et éviter d'augmenter les barrières à l'entrée**.

Pour toutes ces raisons, **lorsque la décision de réglementer est prise, les efforts des gouvernements devraient intégrer de fortes mesures de transparence, de correction et de responsabilisation**. Ces mesures permettent aux décideurs et aux autres parties prenantes concernées de comprendre si les réglementations relatives au contenu fonctionnent comme prévu, y compris en évaluant les activités et l'efficacité des organes de contrôle ou d'application non élus. Lorsque l'expérience démontre que la réglementation du contenu ne fonctionne pas comme prévu, les gouvernements doivent reconnaître et rapidement corriger les problèmes qui se posent.

RECOMMANDATIONS

LÉGALITÉ

- L'élaboration des lois et des règles devrait être faite ouvertement, de manière participative, en tenant compte de la diversité et de la contribution des experts, sur la base d'analyses empiriques et accompagnée d'évaluations d'impact.
- Dans la mesure où des pouvoirs réglementaires et discrétionnaires substantiels sont délégués à des organismes indépendants, créer des mécanismes de surveillance et de responsabilisation fiables pour veiller à ce que ces organismes agissent conformément à l'intérêt public et aux obligations internationales.
- Veiller à ce que les lois publiques soient « formulées avec suffisamment de précision pour permettre à un individu de contrôler sa conduite en conséquence ».
- Les approches qui établissent des critères limitatifs clairs et laissent à un juge le soin de déterminer quand ces critères sont respectés sont les plus appropriées.
- Définir clairement et précisément ce qui est interdit, ainsi que les personnes qui peuvent être tenues responsables de l'échec du respect de l'interdiction.
- Définir des attentes claires pour une action responsable de l'entreprise en ce qui concerne les signalements de contenus illégaux.
- Veiller à ce que la loi exige transparence, supervision et recours, de manière à éviter de « conférer un pouvoir discrétionnaire absolu pour la restriction de la liberté d'expression aux personnes chargées de son exécution ».

LÉGITIMITÉ

- Veiller à ce que le contenu interdit entre dans l'un des « objectifs légitimes » énumérés à l'article 19, paragraphe 3, du PIDCP.
- Veiller à ce que le contenu controversé et offensant ne soit pas interdit simplement parce qu'il met certains publics mal à l'aise.
- S'assurer que le contenu autorisé dans les contextes analogiques est également autorisé sous forme numérique.

NÉCESSITÉ

- Fournir un support empirique et une clarté argumentative pour établir « un lien direct et immédiat entre l'expression et la menace ».

- Mener une délibération attentive, publique et participative pour s'assurer que les lois sont appropriées pour remplir leur fonction de protection, sont l'instrument le moins intrusif parmi ceux qui pourraient remplir leur fonction de protection et sont proportionnées à l'intérêt à protéger.
- Examiner minutieusement quels types de services privés et à quelles couches de la pile technologique sont les mieux placées pour répondre aux préoccupations particulières en cause, en concentrant les efforts là où les risques et les impacts les plus importants se produisent et peuvent être traités le plus efficacement possible.
- Accueillir une gamme variée de modèles d'affaires et de capacités. Examiner l'incidence que les exigences pourraient avoir sur les start-ups et les entités plus petites, ainsi que les effets imprévus qu'elles pourraient avoir sur la politique de concurrence.
- Fournir des indications claires quant aux caractéristiques précises du contenu et des circonstances qui exigent une action rapide ou importante.
- Élaborer des normes pour une modération appropriée du contenu fondée sur les concepts traditionnels de la primauté du droit tels que la transparence, le respect du droit et les recours.
- Permettre la variation et l›expérimentation de l›approche, y compris la « mise en quarantaine » et le « déclassement » du contenu. Fournir des moyens de se prémunir contre les mauvaises utilisations intentionnelles et les conséquences non intentionnelles des mesures de suppression de contenu, y compris les mécanismes d›appel et de recours.
- Exiger des tribunaux qu›ils statuent sur les contenus illégaux et qu›ils fixent des attentes claires pour les intermédiaires, en concentrant la surveillance sur l›aide à la conformité et l›identification des défaillances systémiques.
- Veiller à la mise en place de mécanismes correctifs fiables pour les utilisateurs dont le contenu est restreint afin d›éviter l›incitation à l›autocensure et à la suppression excessive. Intégrer des vérifications périodiques ou des ré-autorisations dans la loi, en veillant à ce qu›elles demeurent pertinentes et conformes à l›évolution des normes et des technologies.

CONFIDENTIALITÉ

- Réfléchir de manière créative pour faciliter la responsabilisation de ceux qui violent la loi tout en continuant à renforcer la protection de la vie privée pour tous.
- Reconnaître que l›anonymat et le pseudo-anonymat peuvent aider les utilisateurs vulnérables à se protéger du harcèlement.
- Reconnaître la valeur d›un chiffrement fort pour protéger les utilisateurs, les services TIC et l›écosystème des TIC.
- Veiller à ce que les autorités respectent les obligations en matière de procédure régulière et les niveaux de preuve avant de demander des données sensibles sur les utilisateurs.