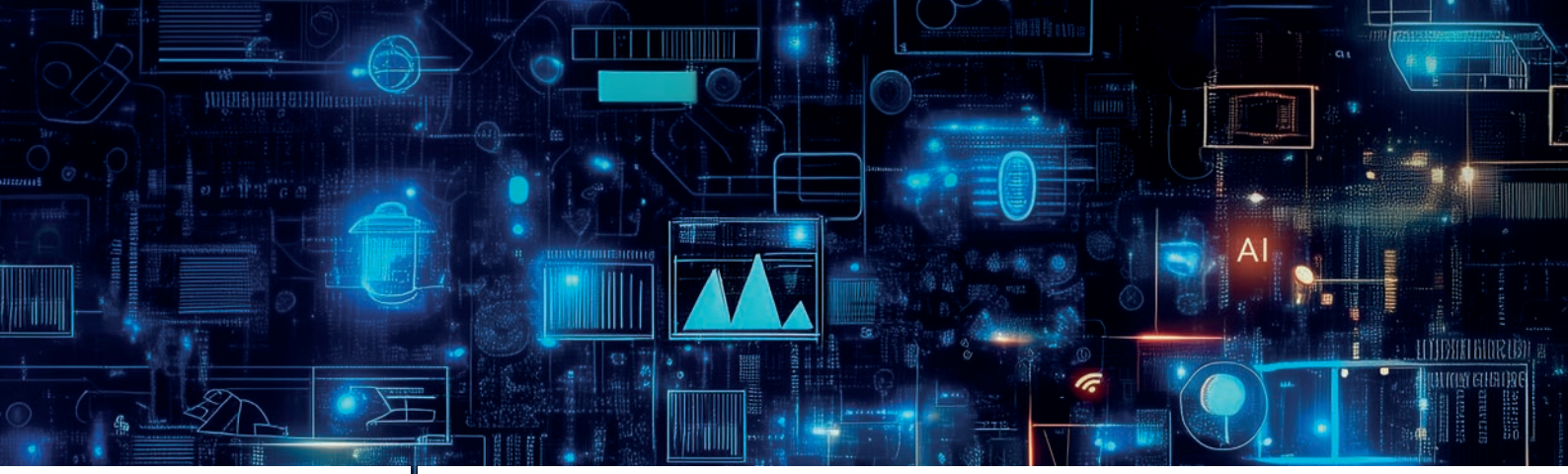

COLLECTION
DÉBATS ET DOCUMENTS
OCTOBRE 2024

37

TECHNOLOGIES ÉMERGENTES

DÉFIS SOCIÉTAUX ET DÉMOCRATIQUES

LUCIE DU PASQUIER (ED.)

FONDATION
JEAN MONNET
POUR L'EUROPE

Table des matières

Il faut responsabiliser les intermédiaires d'information et les fournisseurs de services informatiques

Sylvain Métille
Professeur en protection des données et droit pénal informatique à l'Université de Lausanne
Avocat au barreau (HDC)
Août 2024

Depuis l'invention du web par Tim Berners-Lee en 1989[130], les services en ligne ont beaucoup évolué. L'idéal de liberté et de partage des connaissances en ligne semble bien loin. Face au volume d'informations disponibles, le plus souvent de qualité variable, l'internaute ne voit plus que ce qui lui est proposé et présélectionné par les intermédiaires d'information, qu'il s'agisse de moteurs de recherche, de réseaux sociaux, de plateformes multimédias, de services de microblogging ou de messagerie instantanée, ou d'autres services hybrides.

Ces intermédiaires permettent et facilitent l'accès à l'information. Ils jouent dans ce sens un rôle positif, y compris s'agissant de la libre formation de l'opinion nécessaire au bon fonctionnement de tout espace démocratique. Ils permettent par exemple à un journal local de viser une audience bien plus large sans frais ou à un individu de publier des contenus sans qu'il ne dispose lui-même de la moindre infrastructure technique.

Contrairement aux fournisseurs d'hébergement du début du web, qui se contentaient de mettre à disposition un espace sur lequel d'autres fournissaient leur contenu, les intermédiaires d'information actuels disposent de capacités beaucoup plus étendues sur les contenus qu'ils rendent accessibles. Ce sont eux qui peuvent notamment décider quel contenu mérite d'être vu par qui, quel contenu doit être promu, ou au contraire quel contenu sera perdu au milieu de milliers d'autres.

Par exemple, un moteur de recherche ne donne pas simplement accès à des contenus fournis par des tiers. Il propose de reformuler la question, reprend directement certains extraits d'autres sites sur sa page d'accueil pour répondre à la question posée sans quitter le site du moteur de recherche, ou au contraire propose de visiter certains sites en particulier parce qu'ils sont jugés plus pertinents ou parce qu'ils font l'objet de la publicité payée la plus chère.

Bien loin de la conception du début du web de simples conduits passifs et neutres de l'information, ces intermédiaires sont devenus de véritables portes d'accès à l'information[131]. Ces intermédiaires jouent un rôle fondamental dans notre société, mais ils restent très peu encadrés, en particulier s'agissant du contrôle de l'information. Les dérapages sont pourtant bien connus, comme l'ont tristement montré en 2017 déjà les conséquences de la propagation de contenus nocifs anti-Rohingyas au Myanmar, amplifiée par les algorithmes de Facebook[132].

Le manque de transparence dont font preuve certains intermédiaires, notamment concernant les règles avec lesquelles il est décidé de supprimer ou maintenir un compte ou un contenu, reste tout aussi inquiétant. X (anciennement Twitter) l'a démontré avec la fermeture (puis la réouverture) du compte de Donald Trump, ou encore avec le faible nombre de personnes en charge de la modération des contenus[133].

Au vu de leur position dominante et de la prolifération de certains contenus portant grandement atteinte à la sphère publique comme la désinformation ou les discours de haine, le législateur de l'Union européenne s'est doté d'un « paquet législatif » sur les services numériques, qui inclut le règlement sur les services numériques (DSA) et le règlement sur les marchés numériques (DMA), pour mieux responsabiliser ces acteurs.

130 Concernant l'histoire du web, voir par exemple : https://home.cern/fr/science/computing/birth-web.

131 Riordan Jaani, The Liability of Internet Intermediaries, thèse, Oxford 2016, p. 8.

132 Voir par exemple : https://www.amnesty.org/fr/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/.

133 La Commission européenne a d'ailleurs ouvert une procédure formelle à l'encontre de X en particulier sur ces questions de transparence et de modération des contenus. Communiqué de presse de la Commission européenne du 18.12.2023, disponible ici : https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_6709.

Afin de mieux lutter contre la prolifération des contenus illicites, le DSA prévoit désormais un certain nombre d'obligations de transparence à charge des grandes plateformes en ligne, qui viennent également renforcer les droits des utilisateurs. Le DMA impose quant à lui des obligations particulières à certaines entreprises qualifiées de « contrôleur d'accès » (*gatekeeper*), compte tenu de leur puissance économique, pour éviter les dérives du marché. Jusqu'à présent, la Commission européenne a désigné six entreprises de contrôleur d'accès, à savoir Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta (Faceboook) et Microsoft[134].

La responsabilité des différents acteurs est une problématique plus large, qui concerne l'ensemble du monde numérique. Elle a suscité quelques débats il y a une dizaine d'années, avec les projets de « personnalité » pour les robots, ce qui devait permettre, en échange de la souscription d'une assurance responsabilité civile, d'exonérer de toute responsabilité les concepteurs de ces machines[135]. Ces propositions n'ont pas abouti en raison du peu de robots utilisés par le grand public, mais aussi par crainte de voir des concepteurs complètement immunisés.

La question ne va pas manquer de redevenir actuelle, étant donné les développements technologiques récents et la démocratisation du recours à l'intelligence artificielle, dont notre compréhension n'est encore qu'à ses balbutiements.

Même si le législateur suisse n'a pas encore pris de décision sur la manière dont il souhaite encadrer le recours à l'intelligence artificielle[136], le droit de la protection des données impose déjà des obligations de transparence et de contrôle humain en cas de décision automatisée (art. 21 LPD). Il ne fait non plus guère de doute que celui qui utilise un outil d'intelligence artificielle en est responsable.

En mars, le Parlement européen a adopté le règlement sur l'intelligence artificielle (AI Act), qui prévoit une appréciation des risques en distinguant quatre catégories de systèmes d'intelligence artificielle. Ceux qui présentent un risque inacceptable seront interdits. Ceux à haut risque devront respecter de nombreuses exigences. Ceux présentant des risques limités seront essentiellement soumis à une obligation de transparence, tandis que ceux qui ne présentent qu'un risque minime n'auront aucune obligation particulière à respecter.

Actuellement, et d'une manière qui serait totalement inconcevable dans d'autres domaines, le monde informatique s'est habitué à des exclusions massives de responsabilité. Si un objet est vendu avec une garantie obligatoire de trois ans contre les défauts (art. 197 CO), il est standard qu'un logiciel, même coûteux et développé sur mesure, ne soit livré qu'avec une garantie de quelques jours. Il faut alors souscrire à un contrat séparé de maintenance, par lequel le fournisseur s'engage, contre le paiement de redevances évidemment, à corriger les erreurs rencontrées. De même, il s'agit le plus souvent d'une obligation de moyens (ou de meilleurs efforts) et non d'une obligation de résultat.

L'internaute s'est aussi habitué à consommer des contenus rapidement et surtout gratuitement. Cette gratuité n'est toutefois qu'apparente. L'internaute paie quand même, mais pas en argent, par exemple en acceptant de visionner des publicités, de partager ses données personnelles, ou encore de tester et d'entraîner un service qui n'est pas encore abouti. De plus, le service lui est en général fourni « tel quel », soit sans garantie ni responsabilité, soit avec une responsabilité très fortement limitée (parfois à quelques francs). Mais tout cela semble acceptable, puisque le service est gratuit. Qui oserait exiger des garanties pour quelque chose qu'il reçoit à bien plaire ? Et même quand il paie une licence, les conditions lui sont très défavorables et les cas de responsabilité demeurent bien limités.

Pourtant, cela pourrait changer. La Commission européenne veut par exemple imposer des obligations de cybersécurité communes pour tous les appareils connectés avec la loi sur la cyberrésilience[137], et adapter la directive sur responsabilité du fait des produits à l'ère numérique[138]. Dans le même sens, l'administration Biden a fait part de son intention de proposer une législation qui

134 Communiqué de presse de la Commission européenne du 06.09.2023, disponible ici : https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_4328.

135 C'était ce que prévoyait le point 59 let. c) de la Résolution du Parlement européen du 16.02.2017. Cette dernière est disponible ici : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017IP0051.

136 Le Conseil fédéral a chargé le DETEC d'élaborer un aperçu des approches réglementaires possibles pour la fin de l'année 2024. Communiqué de presse du Conseil fédéral du 22.11.2023, disponible ici : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98791.html.

137 Proposition de Règlement du Parlement européen et du Conseil du 15.09.2022 concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 (COM (2022) 454 final).

138 Proposition de Directive du Parlement européen et du Conseil du 28.09.2022 relative à la responsabilité du fait des produits défectueux (COM (2022) 495 final).

rendrait notamment responsables les entreprises qui vendent des logiciels qui ne sont pas pourvus d'une cybersécurité suffisante[139].

Même si ces innovations proviennent essentiellement de réglementations étrangères, il est fort à parier qu'elles trouveront également leur place en droit suisse. Non seulement celles-ci ont souvent conduit indirectement le législateur suisse à adopter des dispositions similaires, mais leur large champ d'application extraterritorial peut aussi toucher de nombreux acteurs sis en Suisse[140]. Enfin, comme nous l'avons vu le législateur suisse ne reste pas totalement impassible sur ces questions, et il conviendra en particulier de suivre les développements liés aux projets de réglementations sur les grandes plateformes de communication[141], et celui relatif à la réglementation de l'intelligence artificielle[142].

La protection des données personnelles et des droits fondamentaux des internautes est assez bien prise en compte par les lois récentes de protection des données. La Loi fédérale sur la protection des données révisée (LPD) est appliquée en Suisse depuis le 1er septembre 2023, alors que le Règlement général sur la protection des données (RGPD) protège les résidents de l'espace économique européen (EEE) depuis 2018.

Quant au droit pénal, il couvre depuis longtemps la plupart des infractions commises en ligne, notamment les atteintes à l'honneur (173 ss CP), les différentes formes d'escroquerie (146 CP), la soustraction de données et l'intrusion dans les systèmes informatiques (143 ss CP), la pornographie (197 CP), etc. L'ajout récent de l'usurpation d'identité (179decies CP) et prochainement de la pornodivulgation (197a CP)[143] contribuera davantage à améliorer la protection des lésés.

Certaines normes demeurent toutefois lettre morte. Ainsi, la mise à disposition de contenu pornographique à des mineurs constitue un délit pouvant conduire à une peine de prison jusqu'à trois ans[144]. Cette disposition est pourtant systématiquement violée, sans que cela ne suscite de grandes réactions. Certes les mesures de contrôle, qui doivent aussi respecter la sphère privée des internautes, ne sont pas évidentes à mettre en place, mais on pourrait quand même exiger des sites qui proposent de tels contenus qu'ils prennent des mesures adéquates pour respecter la loi et protéger les plus jeunes.

Dans l'ensemble, le droit matériel apparaît malgré tout plutôt satisfaisant et c'est l'application du droit qui doit être améliorée. Si les lois de protection des données garantissent les droits des personnes concernées, l'application de ces lois reste parfois théorique et les personnes concernées doivent agir seules pour faire respecter leurs droits. Une plus grande action des autorités de surveillance serait bienvenue.

Les autorités de poursuite pénale (justice et police) doivent traiter un nombre toujours plus important d'infractions commises dans le cyberespace, alors que leurs moyens n'ont guère été adaptés. La nature essentiellement décentralisée d'Internet et des intermédiaires d'information implique des actes d'enquêtes internationaux et une collaboration avec des États parfois lointains ou dont les préoccupations peuvent fondamentalement différer des nôtres[145].

139 L'administration Biden-Harris a publié en mars 2023 sa stratégie en matière de cybersécurité nationale (NSC). Cette dernière est disponible ici : https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

140 Sury Ursula, Digital Services Act (DSA), Informatik Spektrum 45 2022, p. 266.

141 Communiqué de presse du Conseil fédéral du 05.04.2023, disponible ici : https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/communiques-de-presse.msg-id-94116.html.

142 Communiqué de presse du Conseil fédéral du 22.11.2023, disponible ici : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98791.html.

143 Cette disposition entrera en vigueur le 1er juillet 2024.

144 Art. 197 al. 1 CP.

145 Le Conseil fédéral a dernièrement souligné ce problème dans le contexte des discours de haine en ligne (Conseil fédéral, Discours de haine. La loi présente-t-elle des lacunes ? Rapport du 15 novembre 2023, p. 12).

Bibliographie

AMNESTY INTERNATIONAL. *Myanmar. Les systèmes de Facebook ont promu la violence contre les Rohingyas – Meta doit des réparations*, 29 septembre 2022. Disponible à : https://www.amnesty.org/fr/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

CERN. *La naissance du web*. Disponible à : https://home.cern/fr/science/computing/birth-web

Communiqué de presse de la Commission européenne. *La Commission ouvre une procédure formelle à l'encontre de X au titre du règlement sur les services numériques*, Bruxelles, 18 décembre 2023. Disponible à : https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_6709

Communiqué de presse de la Commission européenne. *Règlement sur les marchés numériques : la Commission désigne six contrôleurs d'accès*, Bruxelles, 6 septembre 2023. Disponible à : https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_4328

Communiqué de presse du Conseil fédéral. *Intelligence artificielle : le Conseil fédéral examine les approches réglementaires*, 22 novembre 2023. Disponible à : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98791.html

Conseil fédéral. *Discours de haine. La loi présente-t-elle des lacunes ? Rapport du Conseil fédéral en réponse au postulat 21.3450 de la Commission de la politique de sécurité du Conseil des Etats du 25 mars 2021*, 15 novembre 2023, 20 pp.

Conseil fédéral. *Intelligence artificielle : le Conseil fédéral examine les approches réglementaires*, 22 novembre 2023. Disponible à : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98791.html

Conseil fédéral. *Grandes plateformes de communication : le Conseil fédéral aspire à une réglementation*, 5 avril 2023. Disponible à : https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/communiques-de-presse.msg-id-94116.html

Règles de droit civil sur la robotique. « Résolution du Parlement européen du 16 février 2017 contenant dess recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103 (INL)) » in. *Journal officiel de l'Union européenne*, 18 juillet 2018, 19 pp. Disponible à : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017IP0051

RIORDAN, Jaani. *The Liability of Internet Intermediaries*, Oxford University Press (Thèse), 2016, 696 pp.

SURY, Ursula. « Digital Services Act (DSA) » in. *Informatik Spektrum*, vol. 45, n° 4, 2022, pp. 265-266

The White House. *National Cybersecurity Strategy*, mars 2023, Washington, 39 pp. Disponible à : https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf