Peut-on censurer tout en respectant la vie privée ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 novembre 2022

https://www.bortzmeyer.org/filtrage-vie-privee.html

C'était le thème d'une réunion pendant l'IETF 115 <https://www.ietf.org/how/meetings/115/> à Londres. Pour censurer sur l'Internet, le censeur doit regarder ce à quoi l'utilisateur voulait accéder, ce qui pose des problèmes de vie privée évidents. Peut-on censurer sans violer la vie privée ?

Le problème était posé sous la forme d'une question technique mais, évidemment, c'est plus compliqué que cela. Avant de détailler tous les aspects, voyons comment fonctionne un mécanisme de censure simple : l'utilisateur veut visiter https://truc-interdit.example/, les équipements intermédiaires sur le réseau voient cette demande, la comparent à une liste de choses interdites et bloquent éventuellement la visite. On peut réaliser cela de plusieurs façons, par exemple par un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> menteur <https://www.bortzmeyer.org/censure-francaise.html> ou par un relais HTTP qui regarde les URL. Peu importe : dans tous les cas, des équipements intermédiaires apprendront qu'on voulait accéder à telle ou telle ressource. C'est ennuyeux pour les droits humains et ça rentre en conflit avec des techniques comme DoT ou HTTPS, qui sont justement là pour empêcher ce genre d'interceptions.

Mes lectrices et lecteurs informaticien·nes peuvent faire une pause ici et se demander comment techniquement réaliser une telle interception sans apprendre l'identité de la ressource à laquelle on voulait accéder. C'est un exercice intellectuellement stimulant. Mais, je le dis tout de suite, le problème n'est pas purement technique. En attendant d'élargir la question, je vous laisse quelques minutes pour réfléchir à une solution technique.

C'est bon, les quelques minutes sont écoulées ? Une solution possible serait, pour le cas du Web, que votre navigateur condense l'URL et envoie cet URL condensé à un service de filtrage qui répond Oui ou Non. Cela préserverait la vie privée, tout en permettant le filtrage. (Oui, il y a quelques détails techniques à prendre en compte, il faut saler pour éviter la constitution de dictionnaires, et il faut canonicaliser pour éviter qu'un malin ne fasse varier les URL pour éviter la détection, etc. Mais ne laissez pas ces détails techniques vous absorber trop longtemps.)

Le vrai problème de cette technique ? Elle nécessite la coopération de l'utilisateur (plus exactement de ses logiciels). C'était le point soigneusement dissimulé par le groupe qui avait organisé cette réunion,

l'Internet Watch Foundation. (Au passage, cette réunion était un "*side meeting*", réunion qui utilise les salles de l'IETF mais qui n'est pas forcément approuvée par l'IETF.) Le titre officiel de la réunion était « "*Is Privacy preserving Web Filtering Possible ?*" » alors qu'en fait le désir n'était pas de filtrer mais de censurer (le filtrage se fait avec le consentement de l'utilisateur, la censure contre son gré). Le présentateur avait introduit la réunion en disant que le but était d'éviter qu'un internaute innocent ne soit exposé contre son gré à des images pédo-pornographiques. Si c'était vraiment le cas, le problème serait simple : un logiciel de filtrage sur la machine de l'utilisateur, comme on fait avec les bloqueurs de publicité. Le cas de la pédo-pornographie est un peu plus complexe car, contrairement aux bloqueurs de publicité, on ne souhaite pas distribuer les listes d'URL bloqués (des pédophiles pourraient les utiliser pour aprendre de nouvelles ressources). Mais ce n'est pas un gros problème, la solution du service qu'on interroge en lui envoyant un condensat de l'URL suffit.

Non, le vrai problème, c'est le consentement de l'utilisaeur. Si vraiment, on veut rendre un service à l'utilisateur, le problème est relativement simple. Si on veut censurer sans l'accord de l'utilisateur, cela devient effectivement plus compliqué. L'argument comme quoi on voulait protéger l'utilisateur contre une exposition accidentelle ne tient donc pas.

L'Internet Watch Foundation a présenté le problème comme purement technique, sachant très bien que les participant·es à l'IETF sont passionné·es de technique et vont sauter sur l'occasion, cherchant des solutions complexes et intéressantes (par exemple du côté du chiffrement homomorphique, la solution miracle souvent citée). Mais on est là dans un cas où la question n'est pas technique, mais politique. Il n'y a aucun moyen magique de censurer sans le consentement de l'utilisateur et en respectant sa vie privée. Le but de l'IWF était probablement justement de montrer qu'il n'y avait pas de solution technique (« on a été de bonne volonté on a soumis, la question à l'IETF ») et qu'il fallait donc censurer sans se soucier de vie privée.

Notons aussi qu'une infrastructure de censure, une fois en place, sert à beaucoup de choses. La pédo-pornographie, par l'horreur qu'elle suscite, sert souvent à couper court aux débats et à mettre en place des systèmes de censure, qui seront ensuite utilisés pour bien d'autres choses.