

Le rôle de l'anonymat dans le cyberharcèlement.

L'anonymat augmente-t-il la violence sur le net?

Nous présenterons ici certains types de cyberharcèlement. Nancy Willard, directrice du Centre pour une Utilisation Sûre et Responsable d'Internet (CSRIU - Center for Safe and Responsible Internet Use) distingue huit formes de cyberharcèlement : le *flaming*, le harcèlement (*harassment*), la dénigration, la mascarade (masquerade), l'*outing*, l'exclusion, le *cyberstalking* et les *cyberthreats*. Parmi ces formes, nous allons en expliciter les principales pour parler du rôle de l'anonymat dans ces formes de cyberharcèlement. Pour mieux organiser ces formes, nous pouvons les diviser en 2 sous catégories : le cyberharcèlement direct et indirect. Le cyberharcèlement direct étant lorsque les harceleurs s'en prennent directement à la victime via de messages ou des envois de contenu alors que le cyberharcèlement indirect est moins avenant mais toujours aussi conséquent.

1. La question de l'anonymat au coeur des débats

Depuis le siècle dernier, un débat sur l'anonymat fait son apparition : est-ce qu'il attiserait la violence sur le net et est-ce qu'il faudrait le lever ? (Ronfaut, 2019). Emmanuel Macron a déclaré en janvier 2019, devant les maires réunis pour le deuxième acte du grand débat national au Palais des congrès de Souillac (Lot), qu'il fallait tendre à une « levée progressive de toute forme d'anonymat » pour une meilleure transparence de l'information sur Internet. Il avait déjà, quelques mois plus tôt, dénoncé un « anonymat devenu problématique », source de « torrents de haine déversés en ligne. ». Mais cette recherche de la « véritable » identité sur Internet est loin d'être française. 89% des internautes adultes américains estiment ainsi que l'anonymat facilite « la cruauté et le harcèlement en ligne », d'après une étude du Pew Research Center, publiée en 2017. Il est intéressant de constater que, dans cette même étude, 54% des personnes harcelées en ligne l'ont été par un inconnu, ou quelqu'un dont l'identité était masquée. Ce qui signifie que, dans 46% des cas, les harceleurs assumaient sa véritable identité. Les internautes n'ont pas forcément besoin de se cacher pour mal se comporter. En 2016, des chercheurs l'université de Zurich se sont intéressés aux commentaires d'un site allemand de pétitions numériques. Leur bilan : les messages violents avaient plus tendance à être publiés sur des comptes avec des vrais noms, car assumer sa véritable identité, même pour propager la haine, signifie que l'on est plus crédible aux yeux des autres.

Lors d'un live Figaro (Figaro Live, 2019), deux intervenants pour et contre cette levée d'anonymat font part de leurs points de vue sur la question.

La première est Rachida Dati, députée européenne et maire du 7^e arrondissement de Paris qui déclare que trop de choses se disent impunément sur internet. Il est trop facile de diffuser des propos haineux. Le second intervenant est Mounir Mahjoubi, secrétaire d'État chargé du numérique explique qu'une levée d'anonymat est presque impossible. Ce qui constitue notre identité numérique, c'est l'adresse IP. Pour ne pas la communiquer nous

pouvons utiliser des navigateur web libre comme TOR ou des VPN. Pour le cas du navigateur TOR, notre ordinateur va décider d'un chemin à prendre « au hasard » parmi des millions d'ordinateurs connectés au réseau Tor. Finalement, le site web avec qui nous communiquons en bout de chaîne ne sait absolument pas qui nous sommes. Il faudrait remonter tous les maillons de la chaîne... ce qui est impossible.

2. Le cyberharcèlement direct

En premier type de cyberharcèlement direct, nous avons le *flaming*. Le *flaming* ou *flamebait* (qui peut se traduire par « propos inflammatoire »), est selon Willard une pratique consistant à poster des contenus éphémères délibérément hostiles, insultants et généralement avec l'intention de créer un conflit sur un groupe de discussion, un forum (sur un site web) ou dans un jeu vidéo. De tels messages sont appelés *flames*, lorsqu'ils forment une séquence d'échange on parle alors de *flame war*. Il s'agit généralement d'une « explication » ou d'une confrontation entre deux ou plusieurs protagonistes, les autres utilisateurs présents dans la salle de discussion interviennent parfois pour essayer d'atténuer les flames. Le *flaming* n'a jamais pour but d'être constructif ou d'éclaircir une situation. Sa motivation n'est pas dialectique, mais plutôt sociale ou psychologique, il n'a pas pour but d'engager une conversation ou une discussion, mais d'atteindre psychologiquement ou d'embêter moralement la personne d'en face. Les « flameurs » essaient de s'imposer par la force, l'intimidation, la dissuasion ou la persuasion plutôt que par la discussion. Dans la définition du harcèlement, nous avons évoqué la notion de répétition. Ici, la répétition n'est pas obligatoire, on pourrait donc se poser la question de savoir si le flaming devrait faire partie du cyberharcèlement. Le *flaming* peut dans certains cas, suivant l'environnement de communication publique, servir d'appât pour alimenter une discussion comportant des propos haineux en ligne (Willard 2011). Un message haineux lancé sur un fil de discussion peut entraîner une cascade d'autre propos violents. Si l'auteur des *flames* est en plus anonyme, la violence des propos peut être encore amplifiée. Un détachement de sa personne par l'anonymat autorise une perte d'humanité et un sentiment de protection pour ne pas voir ses *flames* rattachées à son identité.

Lorsque le *flaming* se réitère, cela devient du harcèlement en réseau (*harassment*). Comme le harcèlement scolaire traditionnel, caractérisé par le caractère répétitif et offensif des actes. Il se définit par l'envoi répété de messages violents via les canaux de communication numériques. C'est ce que Catherine Blaya appelle le lynchage (dans *Les ados dans le cyberspace: Prises de risque et cyberviolence*). Le plus souvent, cette agression se fait sur les réseaux envers des personnes de l'entourage où victimes et agresseurs se connaissent. « Il s'agit de se moquer sans réfléchir aux conséquences pour la victime » (Blaya, 2013). Dans cette forme de cyberharcèlement, l'anonymat n'est pas souvent employé, car ici le but pour les harceleurs est la visibilité comme dans le harcèlement scolaire dit « classique ».

Un type de cyberharcèlement propre au numérique est la *masquerade*. La *masquerade* est une situation où un harceleur se crée une fausse identité pour harceler quelqu'un de façon anonyme. Les harceleurs peuvent soit se créer une fausse identité, soit usurper l'identité de quelqu'un pour envoyer de nouveaux messages haineux. Il y a donc souvent deux victimes

dans le deuxième cas de *masquerade*: la personne harcelée et la personne qui s'est faite usurper son identité.

3. Le cyberharcèlement indirect

Le cyberharcèlement indirect regroupe différents comportements comme la diffusion de rumeurs. Le cyberharcèlement indirect se distingue du direct par la distance entre l'(les) harceleur(s) et le harcelé. Le cyberharcèlement n'est pas forcément constitué ici d'attaques *ad-hominem**, mais il n'en reste pas moins dévastateur pour la victime. Il existe différents types de cyberharcèlement indirect.

Le dénigrement ou (*put-down*) consiste essentiellement à salir la renommée et la réputation d'une personne. Le caractère indirect de ce type de harcèlement vient du fait que les harceleurs n'ont pas nécessairement besoin d'être en contact avec la victime pour salir sa réputation. Cela peut être fait par l'intermédiaire de messages offensants et dégradants postés sur un espace public : des tweets ou sur un mur Facebook, ou par l'intermédiaire de messages envoyés à des personnes en contact avec la victime : familles, amis proches. Willard donne un exemple de *put down*:

« Unknown middle school students created a Web site all about Raymond. On this site, they posted Raymond stories, Raymond jokes, and Raymond cartoons. They posed questions about Raymond's sex life. They invited anyone visiting the site to submit their own comments and had an e-mail link for people to send comments directly to Raymond ».

« Des collégiens inconnus ont créé un site Web sur Raymond. Sur ce site, ils ont posté des histoires et des blagues sur Raymond ainsi que des caricatures. Ils ont posé des questions sur la vie sexuelle de Raymond. Ils ont invité toute personne visitant le site à soumettre leurs propres commentaires et ont créé un lien vers courriel de Raymond pour que les gens envoient leurs commentaires directement à celui ci. »
(traduction)

Cet exemple date de 2007 mais il peut facilement être adapté aux technologies actuelles et aux réseaux sociaux. "Le support numérique est un moyen de spatialiser l'information pour la rejouer dans le temps" (S.Crozat). Il permet donc une diffusion beaucoup plus large des messages dégradants, et engendre des conséquences psychologiques importantes pour les victimes, qui ne peuvent pas savoir qui a eu accès ou non aux rumeurs. De plus, là où changer d'établissement scolaire suffisait généralement à un élevé harcelé pour échapper à ses agresseurs, le support numérique et sa diffusion à grande échelle supprime cette solution. De plus, le support numérique permet au harceleur de rester anonyme, ce qui lui permet de mettre, au moins dans son esprit, une distance entre ses actes et sa personne. De surcroît, les harceleurs anonymes protège sa propre réputation.

Si le dénigrement contient des informations sur la vie sexuelle de la victime, cela peut s'apparenter à de l'*outing*. C'est une pratique visant à mettre la victime dans une détresse profonde, voire à l'humilier. Elle est caractérisée par l'envoi d'informations confidentielles, sensibles ou gênantes. L'emprise psychologique de l'agresseur sur la victime est alors très

importante, puisque qu'il révèle des informations, voir des images, qui appartenait au domaine privé, sur la place publique que sont les réseaux sociaux.

Il semble intéressant d'aborder ici une forme très différente de cyberharcèlement : le *swatting* qui consiste à appeler les forces de l'ordre et de les prévenir d'une fausse situation de crise au domicile de la victime. Le terme de *swatting* fait référence au SWAT (*Special Weapons And Tactics*), groupe d'intervention policier aux Etats-unis (équivalent du GIGN ou de la BRI en France). La victime voit une unité d'intervention arriver à son domicile, la mettre en joue et la maîtriser avant que le *swatting* soit découvert. Pour réaliser cette forme de harcèlement, l'auteur doit disposer d'informations sur sa victime, en premier lieu son adresse. Ce type de harcèlement est développée surtout aux Etats unis dans la communauté des joueurs en ligne. Nicolas Estano, dans Nouvelles technologies et cyberharcèlement : l'exemple du *swatting*, explique que les conséquences psychologiques de ce genre d'action "sont variables" :

« [les victimes] peuvent, après avoir vu les forces de l'ordre intervenir comme si un preneur d'otage était réellement sur les lieux, avoir la perception de s'être fait avoir, mais aussi vivre un réel traumatisme psychologique. Être confronté à un danger de mort qui fait irruption dans l'espace intime et bien réel du sujet est susceptible d'engendrer un (psycho)traumatisme »

De plus, le fait de se sentir sous la menace permanente d'un *swatting* peut rendre la vie des victimes infernales. Les pseudonymes, très développés chez les joueurs, renforcent la violence du harcèlement, puisque la victime est incapable de savoir qui en est l'auteur, bien qu'elle sache qu'elle a déjà joué avec.

Contrairement au *flaming* et au *harassment* présentés plus tôt, des types de cyberharcèlement non inscrits mais partagés. C'est le cas du "happy slapping" ou vidéo lynchage. Cette pratique consiste à filmer ou photographier une agression physique d'une personne à l'aide d'un téléphone portable et à diffuser les images à un certain nombre de personnes. Ces images peuvent être propagées sur la Toile, les réseaux sociaux ou sur Youtube par exemple. Le caractère public du support numérique est ici exploité pour accentuer l'humiliation de la victime.

Article rédigée par Camille Lecossois & Thibault Chassat, mise en page de Xuan Vinh Ho

NOTE

ad-hominem: par lequel on attaque l'adversaire directement dans sa personne (locution latine)

Références

- Willard, Nancy E. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. Research Press, 2007.
- Blaya, Catherine. Les ados dans le cyberspace: Prises de risque et cyberviolence. De Boeck Supérieur, 2013.
- Ronfaut, Lucie. « Être anonyme sur Internet, pour quoi faire? » LEFIGARO, 2019.

- NW, 1615 L. St, Suite 800 Washington, et DC 20036 USA 202-419-4300 | Main 202-857-8562 | Fax 202-419-4372 | Media Inquiries. « Online Harassment 2017 ». Pew Research Center: Internet, Science & Tech (blog), 11 juillet 2017.
- Figaro Live. « Réseaux sociaux : faut-il lever l'anonymat ? », 25 janvier 2019.
- Estano, N. (2019). Nouvelles technologies et cyberharcèlement : l'exemple du swatting. *Criminologie*, 52(2), 13–32.