COMMUNICATION

Comment protéger son image sur les réseaux sociaux

A l'approche des municipales, la réputation numérique des élus et collectivités sur les réseaux sociaux revêt un aspect stratégique. Cette « e-réputation » se construit via une stratégie de communication digitale positive, mais aussi par la surveillance des éléments négatifs. Des leviers juridiques existent pour gérer l'apparition de tels éléments, qu'il s'agisse de commentaires malveillants ou de contenus illicites.

1 LIMITE À LA LIBERTÉ D'EXPRESSION SUR LES RÉSEAUX SOCIAUX

Les limites à la liberté d'expression sont notamment fixées par la loi du 29 juillet 1881 sur la liberté de la presse. La loi du 21 juin 2004 sur la confiance en l'économie numérique a donné une nouvelle jeunesse à ce texte, en étendant son champ d'application à « tout moyen de communication au public par voie électronique », incluant donc les réseaux sociaux. Par principe, toute publication effectuée sur un profil public se trouve donc soumise à l'ensemble des dispositions relatives à la diffamation, à l'injure ou encore à l'incitation à la haine.

Hasthags, retweets et likes abusifs

L'apparition de nouveaux modes de communication en ligne doit conduire les élus et les collectivités à questionner leurs pratiques. Car les hasthags, popularisés sur le réseau social Twitter, constituent une forme d'expression propre et peuvent donc tomber sous le coup de la loi s'ils contiennent des propos illicites (1). De même, le retweet d'un contenu publié par un tiers est assimilé à une reproduction au sens de l'art. 29 de la loi de 1881. Le fait pour un utilisateur de retweeter un contenu illicite implique donc qu'il reprend la publication à son compte, avec toutes les conséquences juridiques associées (2).

Attention aux comptes gérés par des tiers !

L'article 42 de la loi de 1881 prévoit notamment qu'est auteur de l'infraction le « directeur de la publication ». La doctrine estime que le titulaire d'un compte sur un réseau social peut être considéré comme un directeur de publication au sens de la loi, puisqu'il dispose du pouvoir de publier et de retirer toute publication de sa page (3).

Les usagers des réseaux sociaux doivent ainsi prendre conscience qu'ils restent responsables des contenus publiés via leur page ou sur les groupes qu'ils administrent, quelle que soit la personne ayant effectivement rédigé le propos. Cela signifie que les élus doivent attacher une attention toute particulière à la manière dont ils délèguent la gestion de leurs comptes sur les réseaux à leurs collaborateurs. Un élu local a ainsi pu être condamné pour provocation à la haine raciale en raison de propos publiés par des tiers sur sa page Facebook (4).

2 DÉFENDRE SA E-RÉPUTATION

Peut-on bloquer un utilisateur malveillant ?

Certains élus ou collectivités ont pris pour habitude de « bloquer » certains utilisateurs jugés nuisibles en raison des opinions qu'ils expriment. Une telle pratique soulève une question juridique : la page Facebook ou le compte Twitter d'une personne publique ne constituent-ils pas un espace public de discussion devant rester ouvert à tous ?

Les juridictions américaines se sont penchées sur la question, et ont tranché en jugeant que le Président Trump n'a pas le droit de bloquer des personnes qui le critiquent sur Twitter, une telle pratique étant assimilée à une discrimination fondée sur l'opinion (5). Le seul antécédent connu en droit français est une plainte déposée par un journaliste à l'encontre du président de l'Assemblée nationale, ce dernier l'ayant bloqué sur Twitter. D'après nos informations, cette plainte a été classée sans suite. En l'état du droit, aucun exemple de décision venant sanctionner le fait pour un élu de bloquer un utilisateur n'est connu.

Protection du nom de la collectivité

Les collectivités peuvent déposer leur dénomination comme nom de domaine ou comme marque (6). Une solution intéressante car elle offre à la collectivité une voie de recours contre d'éventuelles usurpations ou utilisations abusives de leur dénomination faites par des tiers.

Veille des contenus publiés

Les informations publiées et partagées sur les réseaux sociaux sont, par nature, susceptibles de toucher

rapidement un large public en un temps très court. Il est donc indispensable de mettre en place une veille régulière des propos tenus en ligne sur une personne donnée, si besoin en ayant recours à des systèmes d'alerte automatisés comme Google Alerts. Une telle vigilance permettra de réagir vite à l'apparition d'un contenu problématique.

3 RÉAGIR À UNE MISE EN CAUSE EN LIGNE

Face à un contenu critique ou potentiellement abusif, le premier niveau de réponse possible consiste simplement à répondre et à contre-argumenter sur les réseaux sociaux. Une stratégie de communication réactive et audacieuse peut permettre de contrer une publication défavorable, voire de la renverser à son avantage. On se souvient ainsi de l'exemple de l'ex-région Picardie, qui s'était vue abondamment moquée en 2012 sur les réseaux sociaux pour avoir utilisé des photos de Californie dans le cadre d'une campagne d'affichage supposée vanter ses atouts viticoles. La région avait réagi très vite et avec humour, parvenant ainsi à transformer le « bad buzz » en opération de communication réussie.

L'obligation d'un droit de réponse

Afin de répondre directement en ligne, la plupart des réseaux sociaux permettent aux utilisateurs de commenter ou de répondre sous la publication d'un contenu. Si une telle fonctionnalité n'existe pas, par exemple sur les blogs de groupes politiques locaux, la loi du 21 juin 2004 fait obligation au site de publier un droit de réponse, sur simple demande de la personne mise en cause. En pratique, cette demande doit être formulée par courrier recommandé avec accusé de réception dans les trois mois de la publication, sans être plus long que le message qui l'a provoqué et dans la limite de 200 lignes.

Dans le cadre de la rédaction de ce droit de réponse, il est recommandé de ne pas citer expressément le nom de la collectivité ou de l'élu mis en cause mais d'utiliser des termes génériques, afin d'éviter la reprise de la réponse sur les moteurs de recherche, ce qui pourrait donner une visibilité accrue au contenu initial.

Obtenir le retrait d'un contenu illicite

Les éditeurs des réseaux sociaux ont généralement mis en place des dispositifs internes de signalement de propos abusifs. Le signalement d'un contenu illicite ou inapproprié par ce biais constitue une méthode efficace pour obtenir rapidement son retrait effectif. Il est recommandé d'être précis sur les raisons et les fondements juridiques de la demande, ce qui augmente les chances d'être pris au sérieux par les modérateurs du site. Si ce signalement reste sans effet, l'article 6 de la loi du 21 juin 2004 prévoit une procédure de notification de l'existence d'un contenu illicite à l'hébergeur, c'est-à-dire à la société qui met à disposition du public les espaces de stockage des contenus qui sont publiés.

A la suite d'une telle notification, qui doit remplir des conditions de formes (alinéa 5 de l'article), l'hébergeur est tenu de procéder au retrait du contenu illicite. A défaut, il expose sa responsabilité civile et pénale. En pratique, les coordonnées de l'hébergeur sont généralement disponibles dans l'onglet « mentions légales » du site web.

En dernier recours, il est envisageable d'introduire une action en justice pour obtenir le retrait d'un contenu illicite, par la voie d'une procédure d'urgence. Ce mode d'action implique toutefois des délais procéduraux qui peuvent être assez longs et qui nous paraissent peu adaptés à la volatilité des réseaux sociaux.

Obtenir le déréférencement d'un contenu avec données personnelles

Le règlement européen sur la protection des données personnelles, du 27 avril 2016 prévoit le droit au référencement d'un contenu contenant des données personnelles, c'est-à-dire toute information se rapportant à une personne identifiée ou identifiable. Il ne s'agit donc pas ici d'obtenir la suppression d'un contenu à la source, mais que des données personnelles n'apparaissent plus dans les résultats d'un moteur de recherche en ligne. Cette solution peut s'appliquer au cas d'une personne qui aurait constaté qu'une recherche sur son nom effectuée sur Google renvoie vers des informations privées la concernant. En pratique, une telle demande doit être effectuée via les formulaires types disponibles auprès des différents moteurs de recherche. En l'absence de réponse dans un délai d'un mois – trois mois en cas de demande complexe –, il est alors possible de saisir directement la Commission nationale informatique et libertés (Cnil) de la demande de déréférencement.

(1) TGI Paris, 24 janvier 2013, n° 13/50276 UEJF / Twitter Inc.

(2) Réponse du ministère de la Justice – JO Sénat 07/04/2016.

(3) « Presse – La liberté d'expression face aux réseaux sociaux », Etude par Benoît Auroy et Elie Stelle, Droit pénal n°6, juin 2017.

(4) Cass. Crim. 17 mars 2015, n° 13-87922.

(5) 2d US Cour of Appeal, Case 18-1691, 7 septembre 2019.

(6) CA Paris, 12 décembre 2017, n° 06/20595.

À NOTER

Si notre analyse détaille les règles existantes à ce jour, le droit en la matière est en pleine évolution, comme en atteste la récente proposition de loi visant à lutter contre les contenus haineux sur Internet, actuellement en discussion au Parlement.

Par Ali Derroulche, avocat associé, et **Olivier Planaud,** avocat collaborateur, cabinet Claisse et associés

RÉFÉRENCES

- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Loi du 29 juillet 1881 sur la liberté de la presse