DISCOURS HAINEUX, COMMUNICATIONS PUBLIQUES ET TECHNOLOGIES DE COMMUNICATIONS DE POINTE

Le paragraphe 319(1) du *Code criminel* dispose que les déclarations haineuses proférées dans un endroit public constituent une incitation à la haine et, par conséquent, une infraction. Le paragraphe 319(2) du *Code* interdit de promouvoir volontairement la haine « autrement que dans une conversation privée ». Selon M. Paul Groarke[1], membre du Tribunal canadien des droits de la personne (TCDP), l'article 13 de la *Loi canadienne sur les droits de la personne* vise à supprimer les aspects dangereux de propos tenus en public. Puisque seuls les discours haineux diffusés publiquement sont considérés comme illégaux au Canada, les tribunaux, dont le TCDP, doivent évaluer les technologies de communications, nouvelles et émergentes, ainsi que les applications servant à transmettre les contenus haineux afin de vérifier si les communications qui en résultent sont suffisamment publiques pour que le *Code criminel* ou la *Loi canadienne sur les droits de la personne* s'applique.

Le présent document examine les critères établis par le TCDP pour l'évaluation des communications publiques transmises par des moyens technologiques. Cet examen résume les principes généraux qui ont permis jusqu'ici au TCDP d'évaluer les technologies et les applications nouvelles, et qui devraient lui servir de guide lorsque se présentent devant lui des propagateurs de discours haineux utilisant ces nouvelles technologies. De plus, l'évaluation de l'incidence des communications publiques permettra aux entreprises qui fournissent des services liés à ces technologies et à ces applications de définir leur rôle relativement à la réduction de l'exposition du public aux contenus haineux communiqués ou rendus accessibles à l'aide de leurs services.

ANDREA SLANE
Andrea Slane est membre associée du cabinet Osler, Hoskin & Harcourt s.r.l, où elle pratique le droit de la propriété intellectuelle et des technologies. Elle est aussi professeure adjointe à l'Université de Toronto.

Principes du TCDP sur les communications publiques transmises par des moyens technologiques

L'article 13 de la *Loi canadienne sur les droits de la personne* a été intégré aux autres mesures sur les droits de la personne dans le but de traiter de l'« envoi de messages téléphoniques haineux » par le Western Guard Party[2]. Bien qu'il ait été créé pour examiner un phénomène technologique spécifique, l'article 13 s'applique remarquablement bien aux nouveaux moyens de communications publiques, comme l'indique l'interprétation de son champ d'application par le TCDP. Extraits d'une précédente évaluation de l'article 13 par le TCDP, les quatre principes suivants peuvent facilement s'appliquer à vaste gamme d'innovations technologiques.

1. **Répétition :** L'article 13 interdit les communications téléphoniques *répétées* de messages haineux, ce qui permet de distinguer l'« envoi de messages téléphoniques haineux » d'une conversation téléphonique privée. Dans son examen de l'article 13 au regard de la *Charte canadienne des droits et libertés* dans l'arrêt *Canada (Commission des droits de la personne) c. Taylor*, la Cour suprême du Canada confirme l'article principalement en raison de l'exigence de répétition et appuie le point de vue du TCDP selon lequel ce n'est pas la technologie en

elle-même qui détermine si une communication est privée ou publique, mais plutôt la façon dont elle est utilisée. En d'autres mots, bien que la radio et la télévision s'adressent clairement à de vastes auditoires de manière simultanée, les technologies conçues pour les communications individuelles peuvent également faire partie d'une campagne de communications publiques, puisqu'une communication individuelle répétée équivaut à une communication de masse[3]. Par conséquent, selon ce premier principe directeur, c'est la manière d'utiliser la technologie pour joindre le public, simultanément ou successivement, qui définit une communication publique, plutôt que les caractéristiques de la technologie elle-même.

2. **Accès du public et passivité du communicateur :** Le deuxième principe important, établi par le TCDP et confirmé par la Cour suprême du Canada dans l'arrêt *Taylor*, concerne le fait qu'une personne est jugée responsable de la communication d'un message haineux au public, même si ce message a été simplement mis à la disposition du public et qu'un membre du public doit chercher le message ou y accéder de manière active. Dans le contexte de l'envoi d'un message téléphonique haineux, le message ne peut être entendu que si une personne compose le numéro de téléphone annoncé par le Western Guard Party. Dans l'affaire *Schnell c. Machiavelli Emprize Associates*, le TCDP a respecté ce principe en rejetant l'argument de l'intimé selon lequel le simple téléchargement d'un site Web vers un serveur ne constitue pas un moyen de communiquer avec le public, puisque techniquement, la transmission de l'information n'apparaît pas lors de l'affichage, mais plutôt seulement lorsque quelqu'un visite le site Web[4]. La conclusion du TCDP est conforme à la définition d'« endroit public » à l'article 319 du *Code criminel*, qui se lit ainsi : « Tout lieu auquel le public a accès de droit ou sur invitation, expresse ou tacite[5] ». L'affichage d'un message sur un site Web constitue donc une communication publique, puisque le public a accès aux sites Web, indépendamment du fait qu'une personne doit choisir d'accéder à un site Web pour être exposée à son contenu haineux.
3. **Accès public à l'aide de services de recherche :** L'intimé dans l'affaire *Machiavelli* a également tenté de soumettre l'argument selon lequel un fournisseur de contenu ne peut pas être considéré comme quelqu'un qui communique le contenu d'un site Web au public s'il n'a pas annoncé le site Web ou n'a pas fourni d'une autre manière l'adresse du site à la personne qui y a accédé. L'intimé a ainsi tenté d'établir une distinction entre la situation où des messages sont affichés sur un site Web et les faits de l'affaire *Taylor*, où le Western Guard Party a annoncé le numéro de téléphone à la fois dans des annuaires téléphoniques et en distribuant des feuillets au coin des rues. Le TCDP n'a pas jugé cet argument persuasif, faisant valoir que, en raison de la disponibilité générale des moteurs de recherche, le public peut trouver un site Web sans que le propriétaire ait à en annoncer l'emplacement. Par conséquent, le troisième principe directeur établit que, s'il existe des moyens accessibles par le public de trouver un message, le message constitue une communication publique.
4. **Accès ouvert aux membres ou aux abonnés :** Dans *Warman c. Kyburz*, le TCDP a examiné la situation où le public devrait s'abonner ou s'inscrire à un forum pour être exposé à des messages haineux[6]. L'intimé dans l'affaire *Kyburz* a créé un forum de discussion sur le Web après la fermeture de son site Web. Dans ce forum, il a affiché des messages haineux (de même que des messages contre le plaignant). Comme il s'agissait d'un forum ouvert et que tout le monde pouvait s'y inscrire et lire les messages, le TCDP a considéré que la communication établie dans le forum était publique. Par conséquent, le quatrième principe directeur indique que, si l'inscription est de façon générale ouverte au public, un message transmis dans un forum aux membres seulement constitue une communication publique. Autrement dit, un message ne devient pas une communication privée simplement parce que les destinataires doivent s'inscrire comme membres ou s'abonner.

Évaluation des technologies de communications et des applications nouvelles

Les décisions du TCDP, mentionnées ci-dessus, se fondent sur plusieurs principes solides qui peuvent servir à évaluer d'autres technologies de communications et d'autres applications qui n'ont pas encore fait l'objet

d'une décision du Tribunal. Ces principes sont les suivants :

- Un message transmis de manière répétée au public constitue une communication publique, même si la communication vise un utilisateur ou un grand nombre.
- Un message est communiqué par l'expéditeur, même si le destinataire doit prendre diverses mesures pour y accéder.
- Lorsque le message peut être trouvé par des moyens offerts à tous, il est accessible au public, indépendamment du fait que l'expéditeur diffuse le message de manière active ou qu'il annonce son emplacement.
- Lorsque les messages sont uniquement accessibles par des personnes inscrites ou abonnées à un forum de discussion, cette communication est publique si l'abonnement est de façon générale ouvert au public.

Certaines technologies et applications plus récentes peuvent être plus facilement que d'autres considérées comme des communications publiques. La plupart du temps, la détermination du caractère public ou non reposera sur les faits, comme pour le service de messagerie téléphonique qui a inspiré l'article 13. L'application des principes mentionnés ci-dessus à certaines des technologies et applications suivantes illustrera le processus d'analyse qui sous-tend ces principes.

(a) **Carnets, babillards électroniques, forums de discussion :** Toute communication diffusée à l'aide d'une application permettant à une personne d'afficher des messages que peut lire l'auditoire général d'Internet est clairement une communication publique, puisque les messages affichés sont accessibles par le public[7]. À la suite de l'affaire *Kyburz*, même si une personne doit s'abonner à un carnet, à un babillard électronique ou à un forum de discussion pour lire ces messages, si l'abonnement est ouvert de manière générale au public, la communication est toujours considérée comme une communication publique.

(b) **Pourriels haineux :** L'envoi massif et non sollicité de courriels haineux (c.-à-d. des pourriels haineux) ou de messages texte haineux vers des téléphones cellulaires sera considéré comme une communication publique, conformément à l'analyse de messages transmis à des répondeurs téléphoniques dans l'affaire *Taylor*, malgré que la messagerie texte ou le courrier électronique s'effectue sur une base individuelle.

(c) **Sites Web sécurisés :** Les sites Web dont l'accès requiert l'entrée d'un mot de passe peuvent ou non être considérés comme une communication publique, suivant le processus par lequel une personne du public obtient un mot de passe. À la suite de l'affaire *Kyburz*, si le public peut obtenir de manière générale des mots de passe en se conformant à certains critères d'adhésion, alors la communication établie dans le cadre d'un site Web sécurisé sera également considérée comme une communication publique.

(d) **Messages baladodiffusés :** La baladodiffusion fonctionne selon le modèle éditeur-abonné, de sorte que, toujours conformément à l'affaire *Kyburz*, un message baladodiffusé devrait être considéré comme une communication publique si l'abonnement est généralement ouvert au public. Tant pour les sites Web sécurisés que pour la baladodiffusion, plus le nombre d'abonnés est limité, plus il est difficile de déterminer si la communication est publique ou non.

(e) **Partage de fichiers poste-à-poste :** Lorsque des documents haineux sont rendus accessibles grâce à un service de partage de fichiers poste-à-poste, la communication sera considérée comme publique si, d'une part, le logiciel de partage de fichiers contient une fonction de recherche qui permet aux utilisateurs du programme d'accéder aux documents haineux, ou si, d'autre part, il existe des services de recherche qui permettraient au public de trouver les fichiers. Les logiciels de partage de fichiers populaires, comme Kazaa et Grokster, ont des fonctions de recherche, de sorte que les utilisateurs qui insèrent des documents haineux dans leurs dossiers partagés les communiquent au public, puisque, conformément à l'analyse du TCDP dans l'affaire *Machiavelli*, les documents se trouvant dans des dossiers partagés sont accessibles à toute personne qui les cherche.
Les programmes de partage de fichiers les plus récents, comme BitTorrent, ne comprennent pas de fonctions de recherche comme les programmes de type Kazaa. Par conséquent, les utilisateurs de ces nouveaux programmes qui sont à la recherche de contenu doivent utiliser d'autres moyens (tels les services de recherche indépendants)

pour trouver l'endroit où les documents sont hébergés. Pour déterminer si les communications transmises à l'aide du programme de partage des fichiers BitTorrent sont publiques, il faudra examiner comment est diffusée l'information sur la façon de trouver les documents et qui a accès à cette information.

Rôle du secteur privé dans la réduction de l'accès du public aux documents haineux

Étant donné les paramètres établis par les principes mentionnés ci-dessus pour déterminer si une communication est publique ou non, le secteur privé peut clairement aider à réduire l'accès du public aux documents haineux. Outre la centralisation actuelle des fournisseurs de services Internet qui agissent en définitive comme portes d'entrée vers les communications sur Internet, les fournisseurs d'outils et de services de recherche d'information ainsi que de carnets ou de services d'abonnement peuvent également supprimer des documents, exclure des membres ou s'assurer que certains emplacements ne transmettent pas des résultats de recherche[8].

Comme les fournisseurs de services Internet, ces fournisseurs de services indépendants ne devraient pas généralement être tenus responsables des documents rendus disponibles ou accessibles grâce à leurs services, à moins qu'ils le fassent intentionnellement, avec la volonté de rendre ces documents accessibles. Les fournisseurs de services Internet sont sensibles à l'opinion publique qui les pousse à supprimer rapidement les documents haineux, parce que ceux-ci violent les ententes contractuelles avec les abonnés, telles qu'elles sont définies dans les politiques d'utilisation acceptable. De même, les autres fournisseurs de services devraient être encouragés à faire leur part pour rendre les documents haineux moins accessibles au public et à inclure un tel engagement dans leurs conditions de service ou leurs politiques d'utilisation acceptable.

Bien que les entreprises adoptent de telles mesures de manière volontaire et sur une base individuelle, les conditions de service ou les politiques d'utilisation acceptable servent à informer les utilisateurs des restrictions qu'impose une conduite acceptable ainsi que des conséquences du non-respect de ces restrictions. En limitant l'accès aux documents haineux, les entreprises aideront le programme canadien des droits de la personne à atteindre son objectif de supprimer de tels documents du discours public et participeront à l'effort général visant à contrecarrer l'action des diffuseurs de propos haineux qui continueront certainement à utiliser diverses technologies pour communiquer leurs messages.

Conclusion

En évaluant tout nouveau moyen de communiquer des messages en vertu de ces principes directeurs, le TCDP devrait être constamment en mesure de déterminer jusqu'à quel point un message haineux constitue une communication publique. L'article 13 couvre donc les technologies et les applications futures, puisqu'il s'est avéré jusqu'ici adaptable aux changements technologiques

Notes

1 *Warman c. Warman* (2005), CHRR Doc. 05-531, 2005, TCDP, paragr. 36.

2 D'après le paragraphe 13(1) de la *Loi canadienne sur les droits de la personne* (S.R. 1985, c. H-6), « constitue un acte discriminatoire le fait, pour une personne ou un groupe de personnes agissant d'un commun accord, d'utiliser ou de faire utiliser un téléphone de façon répétée en recourant ou en faisant recourir aux services d'une entreprise de télécommunication relevant de la compétence du Parlement pour aborder ou faire aborder des questions susceptibles d'exposer à la haine ou au mépris des personnes appartenant à un groupe identifiable sur la base de motifs de distinction illicite ».

3 *Canada (Commission des droits de la personne) c. Taylor* (1979), CHRR Doc. 79-001 (TCDP); *Canada (Commission des droits de la personne) c. Taylor* [1990] 3 R.C.S. 892.

4 *Schnell c. Machiavelli and Associates Emprize Inc. (N° 2)*, 2002, 43 C.H.R.R. D/453 (TCDP).

5 *Code criminel,* paragr. 319(7).

6 *Warman c. Kyburz* (N° 2) (2003), 46 C.H.R.R. D/425, 2003, TCDP, paragr. 18.

7 L'affichage de carnets a été l'objet de poursuites pour propagande haineuse devant plusieurs tribunaux, notamment en France et à Singapour. De plus, les sites qui accueillent des carnets peuvent être tenus responsables s'ils refusent d'enlever des affichages offensants puisque la loi sur les libelles diffamatoires les considère comme des diffuseurs et non seulement comme des intermédiaires.

8 Dans certaines provinces et certains territoires, les services de recherche sont déjà soumis à des lois les obligeant à respecter les questions de contenu relativement à la violation des droits d'auteur (et ils seront possiblement bientôt soumis à de telles obligations lorsque le Canada adoptera les futures modifications à la *Loi sur le droit d'auteur*). L'inventeur de BitTorrent, le programme de partage de fichiers, a récemment conclu une entente avec la Motion Picture Association of America pour empêcher la recherche de films protégés par le droit d'auteur à l'aide de son outil de recherche, preuve qu'il est possible de manipuler les résultats d'une recherche dans un tel contexte.